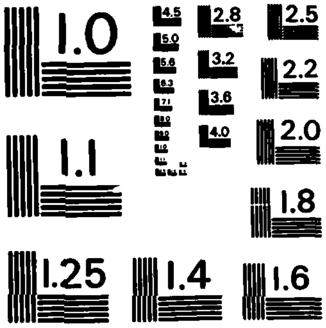
AD-A121 746   FULL-AUTHORITY FAULT-TOLERANT ELECTRONIC ENGINE CONTROL   1/2
SYSTEM FOR VARIAB..(U) GENERAL MOTORS CORP INDIANAPOLIS
IN DETROIT DIESEL ALLISON DI.. L E BAKER ET AL. APR 82
UNCLASSIFIED   DDA-EDR-10895 AFWAL-TR-82-2037   F/G 21/5   NL



1.0
1.1
1.25
1.4
1.6
1.8
2.0
2.2
2.5
2.8
3.2
3.6
4.0
4.5
5.0
5.6
6.3
7.1
8.0
9.0
10

AFWAL-TR-82-2037

12

Full-Authority Fault-Tolerant Electronic Engine Control System for Variable Cycle Engines

Detroit Diesel Allison
Division of General Motors Corporation
P. O. Box 894
Indianapolis, Indiana 46206

June 1982

Final Report for Period September 1979 - April 1982

Approved for public release; Distribution unlimited

Aero Propulsion Laboratory
Air Force Wright Aeronautical Laboratories
Air Force Systems Command
Wright-Patterson Air Force Base, Ohio 45433

NOTICE

When Government drawings, specifications, or other data are used for any purpose other than in connection with a definitely related Government procurement operation, the United States Government thereby incurs no responsibility nor any obligation whatsoever; and the fact that the government may have formulated, furnished, or in any way supplied the said drawings, specifications, or other data, is not to be regarded by implication or otherwise as in any manner licensing the holder or any other person or corporation, or conveying any rights or permission to manufacture use, or sell any patented invention that may in any way be related thereto.

This report has been reviewed by the Office of Public Affairs (ASD/PA) and is releasable to the National Technical Information Service (NTIS). At NTIS, it will be available to the general public, including foreign nations.

This technical report has been reviewed and is approved for publication.

Paul T Adams Jr

PAUL T. ADAMS, JR.
Project Engineer

Lester L Small

LESTER L. SMALL
Technical Area Manager
Controls and Diagnostics

FOR THE COMMANDER

H I Bush

H.I. BUSH
Director
Turbine Engine Division

"If your address has changed, if you wish to be removed from our mailing list, or if the addressee is no longer employed by your organization, please notify AFWAL/POTC, W-PAFB, OH 45433 to help us maintain a current mailing list".

Copies of this report should not be returned unless return is required by security considerations, contractual obligations, or notice on a specific document.

REPORT DOCUMENTATION PAGE

READ INSTRUCTIONS
BEFORE COMPLETING FORM

1. REPORT NUMBER
AFWAL-TR-82-2037

2. GOVT ACCESSION NO.
AD-A121 746

3. RECIPIENT'S CATALOG NUMBER

4. TITLE (and Subtitle)
Full-Authority Fault Tolerant Electronic Engine Control Systems for Variable Cycle Engines

5. TYPE OF REPORT & PERIOD COVERED
Final Report
1 Sept. 1979-30 April 1982

6. PERFORMING ORG. REPORT NUMBER
EDR-10895

7. AUTHOR(s)
L. E. Baker (SCT)
W. E. Brainard (Delco)
C. E. Curry (DDA)
C. P. Disparte (Delco)
L. J. Dolny (SCT)
R. E. Fleming (SCT)
D. E. Warner (DDA)

8. CONTRACT OR GRANT NUMBER(s)
F33615-79-C-2002

9. PERFORMING ORGANIZATION NAME AND ADDRESS
Detroit Diesel Allison, Div. of General Motors
P. O. Box 894
Indianapolis, Indiana 46206

10. PROGRAM ELEMENT, PROJECT, TASK AREA & WORK UNIT NUMBERS
30660386

11. CONTROLLING OFFICE NAME AND ADDRESS
Aero Propulsion Laboratory (AFWAL/POTC)
Air Force Wright Aeronautical Laboratories (AFSC)
Wright-Patterson Air Force Base, Ohio 45433

12. REPORT DATE
April 1982

13. NUMBER OF PAGES
170

14. MONITORING AGENCY NAME & ADDRESS (if different from Controlling Office)

15. SECURITY CLASS. (of this report)
Unclassified

15a. DECLASSIFICATION/DOWNGRADING SCHEDULE

16. DISTRIBUTION STATEMENT (of this Report)

Approved for public release; distribution unlimited.

17. DISTRIBUTION STATEMENT (of the abstract entered in Block 20, if different from Report)

18. SUPPLEMENTARY NOTES

19. KEY WORDS (Continue on reverse side if necessary and identify by block number)
Digital Engine Control
Fault-Tolerant Engine Control
Engine Control Life Cycle Cost
Electronic Engine Control Systems
Full-Authority Engine Control
Engine Control Reliability

20. ABSTRACT (Continue on reverse side if necessary and identify by block number)

The objective of this program was to develop a design approach for full-authority digital electronic control systems with reliability the primary consideration factor. The approach used in attacking this objective was to identify a baseline full-authority digital electronic control system for an advanced fighter aircraft and then improve on this baseline control with respect to specific goals using redundancy, recovery strategies, and maintenance philosophies. Ambitious (Cont'd. on reverse side)

cont

goals were established for controls-related mission reliability (2.5 mission aborts per million operating hours), mean time between control removals (1800 hours), and fail operational capability. Candidate control designs were evaluated with respect to cost and weight in addition to their ability to satisfy the design goals.

The baseline control system was modularized to yield identifiable components (pumps, thermocouples, actuators, etc.). For these components, reliability and cost information was accumulated. This information was used in computer models to evaluate system reliability and system cost for candidate control designs.

The candidate control designs were derived from the single-strand baseline using selected replication of components; analytical redundancy; various failure recovery strategies (coverage); and various maintenance philosophies. Systems were configured based on extensive consulations with industries promoting fault-tolerant digital control system structures such as the telephone and automotive industries.

Many of these configurations were screened with a Markov-based constant failure rate analysis simulation called the Generalized Reliability and Maintainability Program (GRAMP). From GRAMP came quantitative measures of probability of mission completion, system cost, and system weight for the candidate configurations. A Generalized Reliability and Maintainability Simulator (GRAMS) tested promising configurations from GRAMP, using a time-varying analysis approach based on Monte Carlo techniques. In GRAMS candidate configurations were evaluated for a given aircraft fleet size (1,000 engines) and engine life (7000 hours) to determine total Life Cycle Costs associated with fault-tolerant control systems.

The results of the GRAMP and GRAMS analysis showed necessary cost and weight increases associated with achieving an order of magnitude improvement in mission reliability by using a "fault-tolerant" structure as opposed to the baseline system. To achieve the original goals set forth in the program requires a system which is cost and weight prohibitive using present technology.

FOREWORD

This technical report was prepared by Detroit Diesel Allison (DDA) a Division of General Motors Corporation with the aid of major subcontractors Systems Control Technology (SCT) and Delco Electronics, also a Division of General Motors Corporation. This effort was sponsored by the Aero-Propulsion Laboratory, Air Force Wright Aeronautical Laboratories, Air Force Systems Command, Wright-Patterson Air Force Base, Ohio, under contract F33615-79-C-2002 for the period September, 1979 to April, 1982. The work herein was accomplished under Air Force Project No. 3066, Task 03, Work Unit 86. Mr. Charles E. Ryan, Jr. served as Air Force Project Engineer. Mr. Dennis E. Warner of DDA was technically responsible for the work. Other DDA personnel contributing to this program were Mr. C. E. Curry, Mr. R. C. Boyer, Mr. R. D. McLain, and Ms. S. M. Mussmann. The SCT contingent consisted of the project leader, Ms. Laura Baker, and Ms. L. J. Dolney, Dr. R. E. Fleming, Dr. W. E. Hall, Dr. R. L. DeHoff, Mr. S. N. Bangert, and Ms. R. J. Miller. Delco's efforts were directed by Mr. Charles P. Disparte with the assistance of Mr. W. E. Brainard. Special mention is made of the contribution of Bendix Corporation, Energy Controls Division. Although Bendix was not a subcontractor in this program, Bendix personnel nonetheless provided useful data and consultation services. Individual Bendix contributors included Mr. F. J. O'Keefe, Mr. R. E. Raymond, and Mr. R. W. Conrad. The very helpful technology-transfer support contributed by Dr. Wing N. Toy, of the Bell Telephone Laboratories, Naperville, Illinois, is recognized; as is the technical consultation and critique support rendered by Mr. Harold Ascher of the Naval Research Laboratories.

TABLE OF CONTENTS

Table of Contents (continued)

LIST OF ILLUSTRATIONS

LIST OF TABLES

GLOSSARY OF TERMINOLOGY

actuarial data - statistical information which has been accumulated; in FAFTEEC, this represented failure event histories of engine components.

analytical redundancy - given that a sensor has failed, the ability to recreate the signal normally provided by that sensor with the remainder of the operational sensor set.

binomial experiment - a random event with two associated probabilities (i.e. a coin toss).

burn-in - phenomena often associated with electronic components, where component failure rates improve with time.

cause transition matrix - based on a random event, the coefficients governing transition from one state to another.

closed system - a system for which there is no repair.

confidence interval - an interval in which a value falls with a probability.

coverage - the probability that, for a given redundant system, a failed component in the system can be diagnosed and the system can remain operational.

cumulative distribution - a probability distribution of random events

duplex module - a system containing two identical elements.

fail operational - a system characteristic representing that systems ability to remain active and working even though one of the systems components has failed.

fault tolerant - a system characteristic representing the systems ability to remain operational in the face of system failures.

Hamming error correction code - a method for correcting single bit errors in a digital word relying on parity bits interspersed with data bits; double bit errors can also be detected.

independent components - components for which failure of one does not cause the failure of another.

mean time between failure - a statistical average in units of time (normally hours) representing the frequency with which component failures may be expected.

mean time between unscheduled removal - a statistical average in units of time (normally hours) representing the frequency with which components can be expected to be removed due to failures.

opportunistic maintenance - repair conducted on control system components when the engine is returned to the maintenance facility for other than control system repair.

preventative maintenance - repair of noncritical components in order to bring the system to its original state even though the system may be operational.

redundancy - using two or more items to accomplish the function that could be done by one; in FAFTEEC replication and analytical redundancy were used as the two types of redundancy.

replication - using two or more identical items to accomplish the functions that could be done by one; normal procedure is to have one item be active and the other items be spares; should the active item fail, one of the spares would become active and assume functional responsibility.

scheduled repairs - maintenance events which have been established at certain time intervals; time may represent calendar time, component operating time, number of component operating cycles, etc.

stochastic process - a random procedure.

stochastically deteriorating - a system which cannot improve with time and which experiences random events

time slice simulation - a computer model which analyzes a time variant process by breaking the time period analyzed into intervals (time slices)

triplex module - a system containing three identical elements.

two-fail operational - the ability of a system to sustain two normal component failures and remain active and working.

unscheduled repairs - maintenance events due to component failures.

variance reduction - techniques aimed at improving the confidence level of statistical results.

LIST OF ABBREVIATIONS

A/D	Analog to Digital
ATAMS	Advanced Tactical Attack Manned System
ATES	Advanced Technology Engine Studies
ATF	Advanced Tactical Fighter
BIT	Built in Test
BITE	Built in Test Equipment
BLD	Bleed
BNR	Bell Northern Research
BTL	Bell Telephone Laboratories
BU	Backup
CCU	Configuration Control Unit
CDP	Compressor Discharge Pressure
CDT	Compressor Discharge Temperature
CIP	Compressor Inlet Pressure
CIT	Compressor Inlet Temperature
CEM	Cost Evaluation Model
CFR	Constant Failure Rate
COV	Coverage Value
CPU	Central Processing Unit
CSRM	Coherent System Repair Model
D/A	Digital to Analog
DDA	Detroit Diesel Allison
DE	Delco Electronics
EGT	Exhaust Gas Temperature
EHSV	Electro-Hydraulic Servo Valve
EMI	Electro Magnetic Interference
EMP	Electro Magnetic Pulse
EPROM	Erasable Permanent Read Only Memory
ESS	Electronic Switching System

List of Abbreviations (continued)

FAFTEEC	Full Authority Fault Tolerant Electronic Engine Control
FPMH	Failures per Million Hours
FTMP	Fault Tolerant Multi-Processor
FTSC	Fault Tolerant Spaceborn Computer
GRAMP	Generalized Reliability and Maintainability Program
GRAMS	Generalized Reliability and Maintainability Simulator
HPC	High Pressure Compressor
HPT	High Pressure Turbine
HTF	High Flow Through
I/O	Input/Output
IUS	Inertial Upper Stage
JPL	Jet Propulsion Laboratory
LCC	Life Cycle Cost
LEVP	Level Print
LO	List Options
LOPS	List Options (Print)
LP	Low Pressure
LRU	Line Replaceable Unit
LSI	Large Scale Integration
LVDT	Linear Variable Differential Transformer
MOT	Maximum Operating Time
MPA	Maritime Patrol Aircraft
MRB	Material Review Board
MTBF	Mean Time Between Failure
MTBUR	Mean TIme Between Unscheduled Removal
MTBR	Mean Time Between Repair
MTTF	Mean Time to Failure

List of Abbreviations (continued)

NH	High Pressure Rotor Speed
O&S	Operating and Support
OCM	On Condition Maintenance
ORLA	Optimum Repair Level Analysis
PLA	Power Lever Angle
PMA	Permanent Magnet Alternator
RADC	Rome Air Development Center
RAEEC	Reliability Advancement Electronics Engine Controller
RAM	Random Access Memory
RCM	Reliability Centered Maintenance
RCTEC	Reduced Cost Turbine Engine Concept
REL	Reliability
RFI	Radio Frequency Interference
RFM	Reliability/Feasibility Model
SCCM	Self Checking Computer Module
SCT	Systems Control Technology, Inc.
SFC	Specific Fuel Consumption
SIFT	Software Implemented Fault Tolerant
TMR	Triply Modular Redundant
TNOZ	Nozzle Temperature
USAF	United States Air Force
V/STOL	Vertical/Short Take-Off and Landing Aircraft
V/STOL A	Subsonic Vertical/Short Take-Off and Landing Aircraft
VCE	Variable Cycle Engine
WF	Fuel Flow

SECTION I
INTRODUCTION

Major aircraft engine manufacturers are presently engaged in Advanced Turbine Engine Study (ATES) programs to define the ngines which are to power the advanced aircraft of the late 1980's. The ATES program at Detroit Diesel Allison has identified several candidate engine configurations to best handle the missions for Air-to-Air and Air-to-Ground Superiority Fighters, Maritime Patrol Aircraft (MPA), and Subsonic V/STOL (V/STOL A) aircraft. For the Air-to-Air and Air-to-Ground applications, also known as Advanced Tactical Fighters (ATF), a Maximum Temperature Turbojet has been identified as the prime candidate for satisfying the multi-mission needs.

The Maximum Temperature Turbojet proposed for the ATF is a single-spool Variable Cycle Engine (VCE) capable of modulating airflow as well as fuel flow with the use of engine varible geometry components. The ability of control system engineers to coordinate control functions of these variable geometry components with the standard control task of properly modulating fuel flow was the basis for many studies during the '70's. Thus the VCE control system has been constructed with the aid of control component design, control logic design, and control diagnostic implementation. Although the control functional differences between a VCE and a fixed cycle engine have been identified, addressed, and somewhat resolved, reliability concerns persist. Considerations, including failure rates, safety of flight, availability, and maintainability, surround the replacement of hydromechanical technology with digital electronic technology. Analysis and resolution of these considerations forms the basis of this effort, the Full-Authority Fault-Tolerant Electronic Engine Control (FAFTEEC) program.

The FAFTEEC program was an Air Force contracted effort (F33615-79-C-2002). Detroit Diesel Allison (DDA), a division of the General Motors Corporation, was the prime contractor with subcontracted efforts by Systems Control Technology - SCT (formerly Systems Control Incorporated) and Delco Electronics (DE), Santa Barbara Operations, also a division of General Motors Corporation.

Although not identified as a subcontractor, personnel from the Energy Controls Division of Bendix Corporation provided valuable assistance during this program.

The objective of the FAFTEEC program was to demonstrate a practical approach for designing a representative full-authority fault-tolerant electronic control system. The approach was to blend hardware and software redundancy considerations and provide a reasonable basis for evaluating the critical factors which must influence a design, e.g., cost-of-ownership, performance, weight, reliability, availability and so forth. Figure 1 depicts the approach used in the FAFTEEC program.

As displayed in the figure, a baseline system was defined. Mission, aircraft, and engine requirements as taken from the ATES program dictated the use of the full-authority digital electronic control system designed for DDA's GMA200 series engine. The system was interpreted as a modular arrangement with the individual control components (pumps, actuators, digital controller, etc.) comprising the modules. Reliability information, unit cost information, unit weight information, and unit repair information was accumulated on these components, or in some cases similar components, to permit system reliability, cost, and weight calculations to be made based on this realistic data.

Candidate fault-tolerant redundant control systems were configured consisting of variations to the baseline system with redundancy used on the digital controller, sensors, actuators, and other components to achieve the desired reliability. Redundancy was utilized at various degrees within the digital control unit as well as at the component level based upon a reliability analysis of the baseline system to identify relative reliability, strength and weakness within the system architecture.

A rigorous study of the technology base in the analysis of fault-tolerant digital redundant systems was made covering synthesis, mathematical concepts, verification and effectiveness of existing fault-tolerant systems. A careful analysis of the mathematical tehcniques with special attention to tractability

FAFTEEC PROGRAM APPROACH

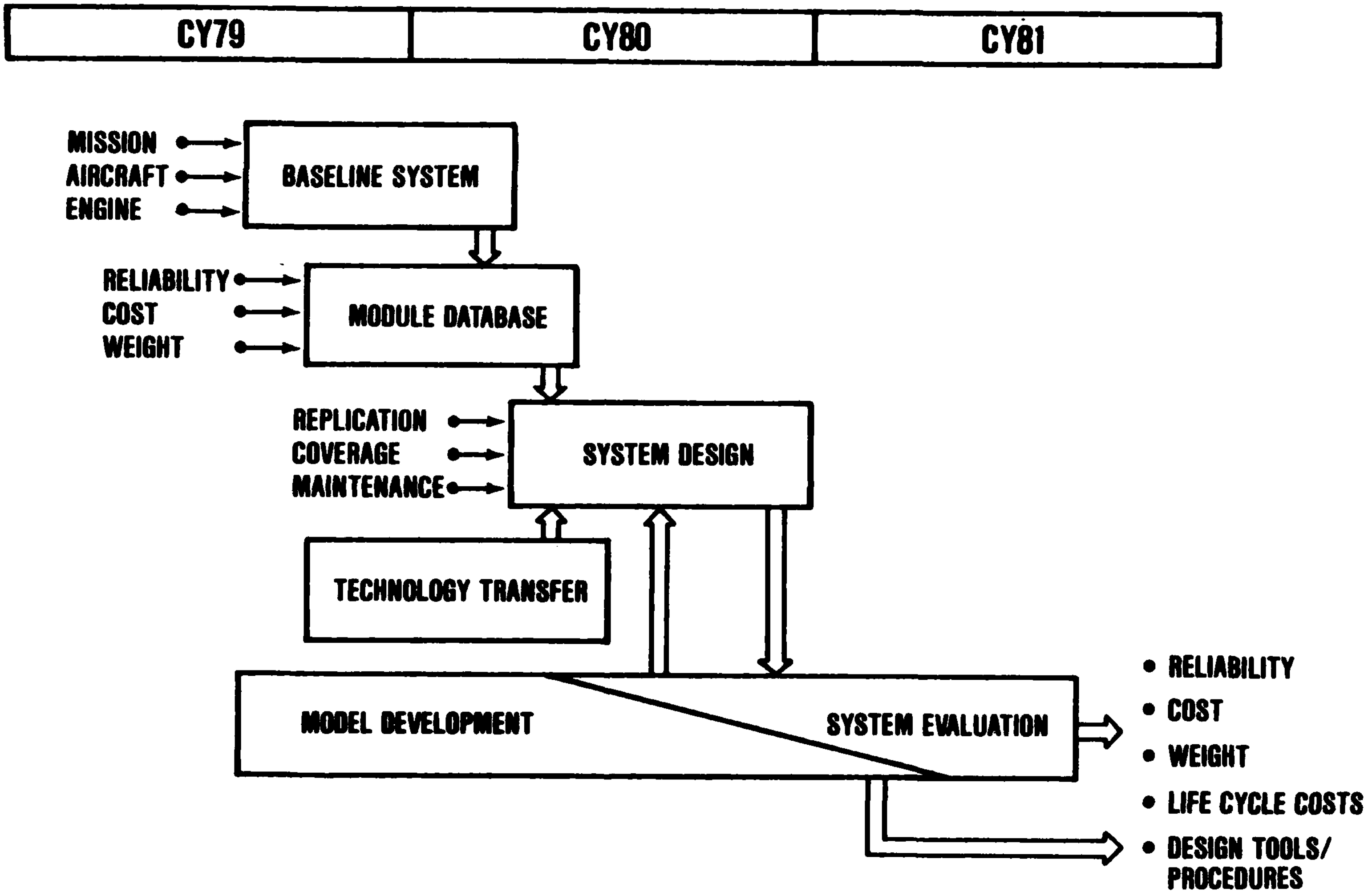


Figure 1. FAFTEEC Design Approach

and validation of assumptions, was conducted prior to the selection of the modeling technique for this program. Special considerations for the analysis include time invariant and variant failure rates, effect of failsafe software, and the inclusion of the effect of maintenance policies while protecting the overall generality of the analysis technique. A time invariant model called the Generalized Reliability and Maintainability Program (GRAMP) was utilized in the initial reliability screening of candidate systems.

Following the screening through GRAMP, representative systems that met the reliability goals were selected for evaluation with reliability and cost models that included time variant characteristics. Then, the lowest cost-of-ownership configurations that met the reliability requirements were identified. For comparison, the baseline system was also evaluated.

This report documents the steps taken in the systematic design approach, the results based on the approach, and design guidelines based on these results. Section 2 summarizes the highlights of the FAFTEEC effort. Sections 3 through 6 document the major tasks within the program as follows:

Section 3	Baseline Control System Description
Section 4	Configuration of Fault-Tolerant Systems
Section 5	FAFTEEC Design Tools
Section 6	Results

The last sections of the report give the Program Conclusions and Recommendations (Section 7).

The FAFTEEC program was an aid in explicitly identifying the reliability considerations which have implicitly been part of the control design process.

SECTION II
SUMMARY

The FAFTEEC program was established to investigate the critical reliability issues of full-authority digital electronic controls systems to be used on advanced military aircraft gas turbine engines. This investigation necessarily evaluated the complete engine control system, comprised of many elements including pumping and metering elements, parameter sensors, geometry actuators, electrical system components and digital computers and ancillary electronic circuitry. This program addresses an overall objective to provide substantial improvement in control system reliability. The specific program objective was to evolve design guidance for future development of digital electronic engine control systems for variable cycle engines using selective redundancy of modules or components combined optimally to provide very high system (mission) reliability with acceptable increases in hardware and software complexity and cost.

Based upon other activities and programs such as Advanced Technology Engine Studies (ATES), Detroit Diesel Allison has defined a Maximum Temperature Turbojet, single spool variable cycle engine for tactical applications (missions). A baseline engine control system was defined to meet overall mission, aircraft and engine requirements. This system is substantially a simplex system. However, redundancy is provided for the speed sensor and the fuel pump, metering valves and nozzles are duplicated to provide separate primary and main fuel systems. This design inherently provides fuel system redundancy during a mission. For this study, the baseline system includes a single digital computer although, in the actual development, the computer is capable of being paralleled.

Using components from the baseline system, redundancy management/fault-tolerant techniques were applied to construct candidate fault-tolerant system configurations subject to a set of design goals. Goals were established to address issues of system effectiveness (failure probabilities, availability), coverage (system recovery), tolerance achievement (recovery time, transient

effects, battle damage), and system overhead. The goals were probability for mission completion of .9999975, fail-operational capability of 2, and system availability (mean time between unscheduled removals) of 1800 hours.

Concepts for achieving fault-tolerance included selective module redundancy, fault recovery strategies, and varied maintenance philosophies. Redundancy techniques applied included replication (duplicate or triplicate hardware configurations to accomplish a given function) and analytical redundnacy (using the remaining operational sensor set to recreate a signal normally provided by a failed sensor). Fault recovery strategies included hardware and software techniques for detecting, isolating, and accommodating a failed system component. Coverage, the probability that a failed module will be identified and proper fault accommodation will be taken, was the quantifiable means used to represent various fault recovery strategies. Maintenance policies considered included conventional On-Condition Maintenance (OCM) practices and Reliability Centered Maintenance (RCM) techniques such as employing Deferred and Opportunistic Maintenance on redundant system configurations.

Contacts outside the aircraft engine development industry were made as part of the Technology Transfer phase of the program. The telephone, aerospace, and automotive industries were consulted to explore methods for achieving high reliability with fault tolerant digital electronics. Valuable sessions were conducted with personnel from Bell Labs, Delco Electronics, Bell Northern, and Bendix. A number of specific design techniques applicable to FAFTEEC were extracted and a specific digital controller architecture was developed. The architecture features a replacement type redundant system having switchable replacement elements for each functional module, a failsafe configuration control unit (CCU), hardware self-checking approach to provide near unity coverage for the critical modules/functions, and software checking for less critical modules. This basic controller architecture was used for all fault-tolerant system designs.

To pursue the design and evaluations of potential fault tolerant system configurations, several analytical models and simulators were developed. Of particular significance are the GRAMP and GRAMS models.

The Generalized Reliability and Maintainability Program (GRAMP) was developed to aid synthesis of fault tolerant configurations. GRAMP assumes that the control system is comprised of a set of functionally independent modules. It was specially developed to provide the capability to handle repairable systems and analytical redundancy including detection/survey strategies. GRAMP includes a procedure to systematically identify and quantify design parameters that actively drive system reliability and maintainability. Additionally, GRAMP provided the desirable characteristic of being able to evaluate a large number of test configurations at low cost.

The Generalized Reliability and Maintainability Simulator model (GRAMS) was a second reliability evaluation tool developed and used in the FAFTEEC program. GRAMS permitted evaluation of more detailed maintenance policies plus a time varying analysis procedure. It also provides the capabilities to evaluate system failure due to temperature events, lightning events, and other normal failure mechanisms, including maintenance events associated with the control system (pre-flight check, MOT, etc.), and penalty costs associated with various maintenance actions.

The primary output of GRAMS are failure probabilities and maintenance events, on a module or system basis. These data were used in a separate Life Cycle Cost Analysis (LCC) procedure to establish O&S costs. The LCC procedure also included evaluation of RDT&E and acquisition (including initial spares) costs.

A critical and fundamental part of the FAFTEEC program was the accumulation and utilization of a realistic data base for the Baseline control system. Using production bases from aircraft engine applications (TF41, F100, F404), other airbourne applications (F16, C141, Titan II), and automotive applications, reliability data sets were accumulated for particular hydromechanical and electronic control components. The information in these data sets included constant failure rates (in failures per million hours) and hazard rate curves (non-constant failure rates) wherever possible. Other pertinent information for these control components included unit cost per component and typical unit repair charge per component. DDA and Bendix supplied data for all non-electronic components while Delco provided the electronics data base.

The baseline engine control system was used as the starting point for defining and evaluating numerous alternate system designs. The baseline system was decomposed into 41 individual functional modules which could be considered independent. At the appropriate functional level these modules were evaluated with respect to replication for fault tolerance and redundancy. Further, at this module level critical issues and characteristics of coverage, fault recovery strategies, maintenance philosophies and procedures and realistic reliability and cost data could be assessed. Primarily using the powerful GRAMP, extensive sensitivity evaluations were made to establish representative system configuration to meet the specified goals. As a result of these preliminary evaluations, several important observations were made. First, it was clear that there are important reliability drivers in the control system other than the electronics; e.g. the actuation systems. Actual field reliability experience with "ancestors" of these components, even assuming substantial improvement and reliability growth, led to the observation that they would be important contributors to unreliability. Second, partly as a result of the foregoing, it was apparent that it would be very difficult to achieve the specified reliability and maintenance goals. Accordingly, it was decided to carry forward in the evaluation two classes of systems, in addition to the Baseline, identified as System 1. These are indicated by Figure 2.

Systems 2 and 3 are constrained to meet the specified mission reliability of 0.9999975. This was achieved by triplexing each module for both systems. In System 2, the module reliabilities were established by the empirical data base and module coverage values were derived in order to meet the goal. Conversely, for System 3, the most realistic assessment of module coverage was established, and module reliability was adjusted to achieve the goal.

Systems 4, 5, and 6 compare the second class of systems which are designed to meet a mission reliability of .9995. This level represents an order of magnitude of improvement over existing systems of comparable functional complexity. This improvement is considered to be achievable with realistic values of component reliability and module coverage. As noted by Figure 2, these 3 systems are labeled approximately in terms of simplex/duplex,

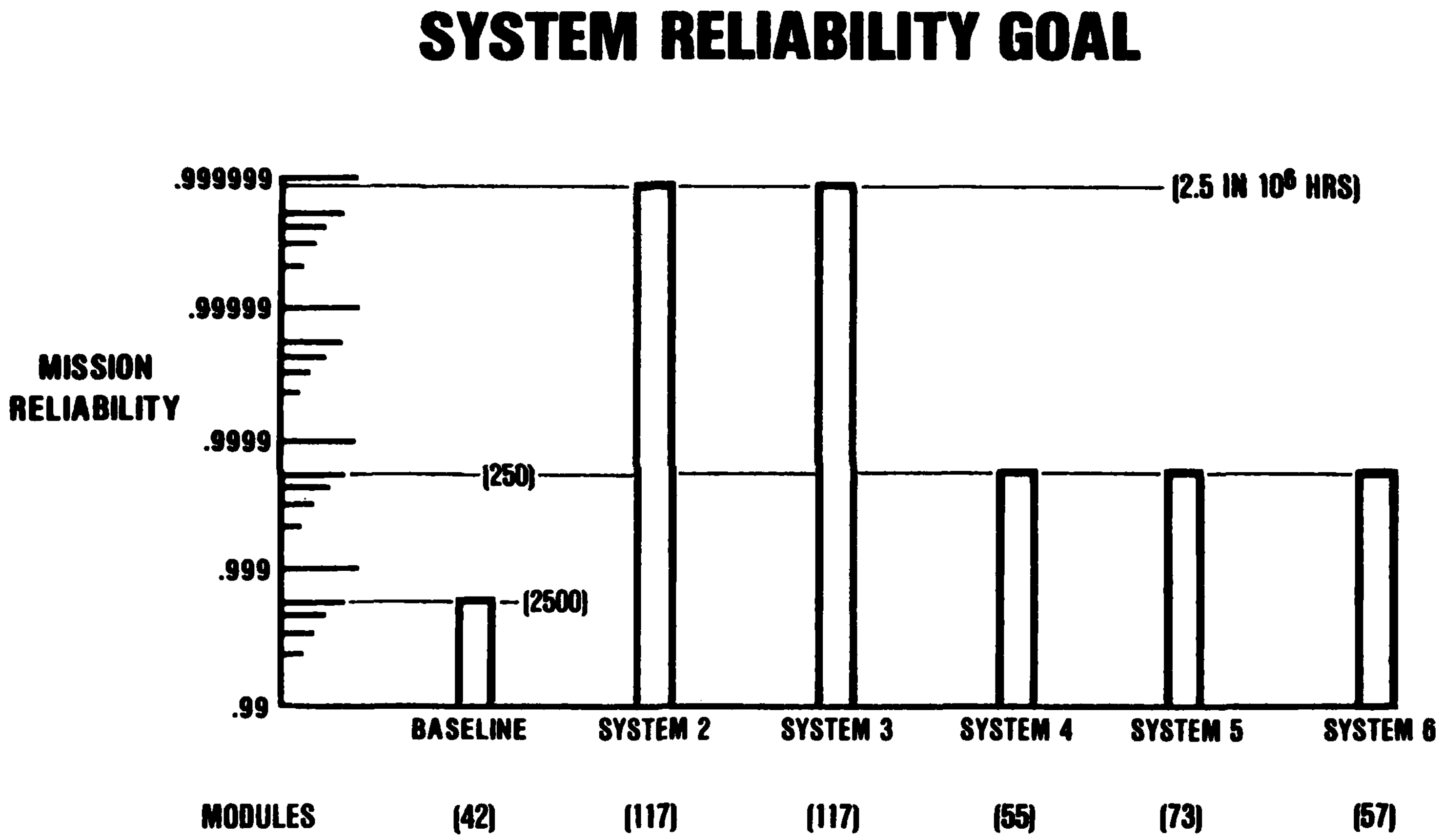


Figure 2. Mission reliabilities addressed by FAFTEEC configurations.

duplex/triplex and duplex. Hardware complexity is more conveniently described on the abscissa by total number of modules shown as 55, 73, 57 for 4, 5, and 6 respectively. These configurations were designed to permit evaluation and sensitivity of coverage and maintenance assumptions. System 4 requires maintenance (no deferred maintenance actions). System 5 provides sufficient hardware replication to permit deferred maintenance. System 6 depends on optimal coverage assumptions and an opportunistic maintenance.

The basic results of the comparative evaluation are shown by Figure 3. In terms of system unit acquisition cost, weight, and system life cycle cost, substantial increases or penalties are evident with large increases in reliability. Even with a more modest reliability goal, increases in cost and weight of 50-100% are projected. Further, it is noted that sensitivity to the maintenance and coverage assumptions associated with Systems, 4, 5, 6 is relatively low, perhaps not significant, so that other considerations such as training might be a strong determining factor.

In summary a Full-Authority Fault-Tolerant Electronic Engine Control system :esign is deemed practical with present technology. Weight and cost penalties are severe enough to penalize the overspecification of the degree of fault-tolerance, i.e. the mission reliability. This FAFTEEC program has produced a systematic approach, using reliability and cost evaluation models, for analyzing the sensitivity of mission reliability, system costs, and system weight to the critical design parameters of module redundancy, coverage , and maintenance philosophy. FAFTEEC, the program, is the first step to evolution of FAFTEEC, the system.

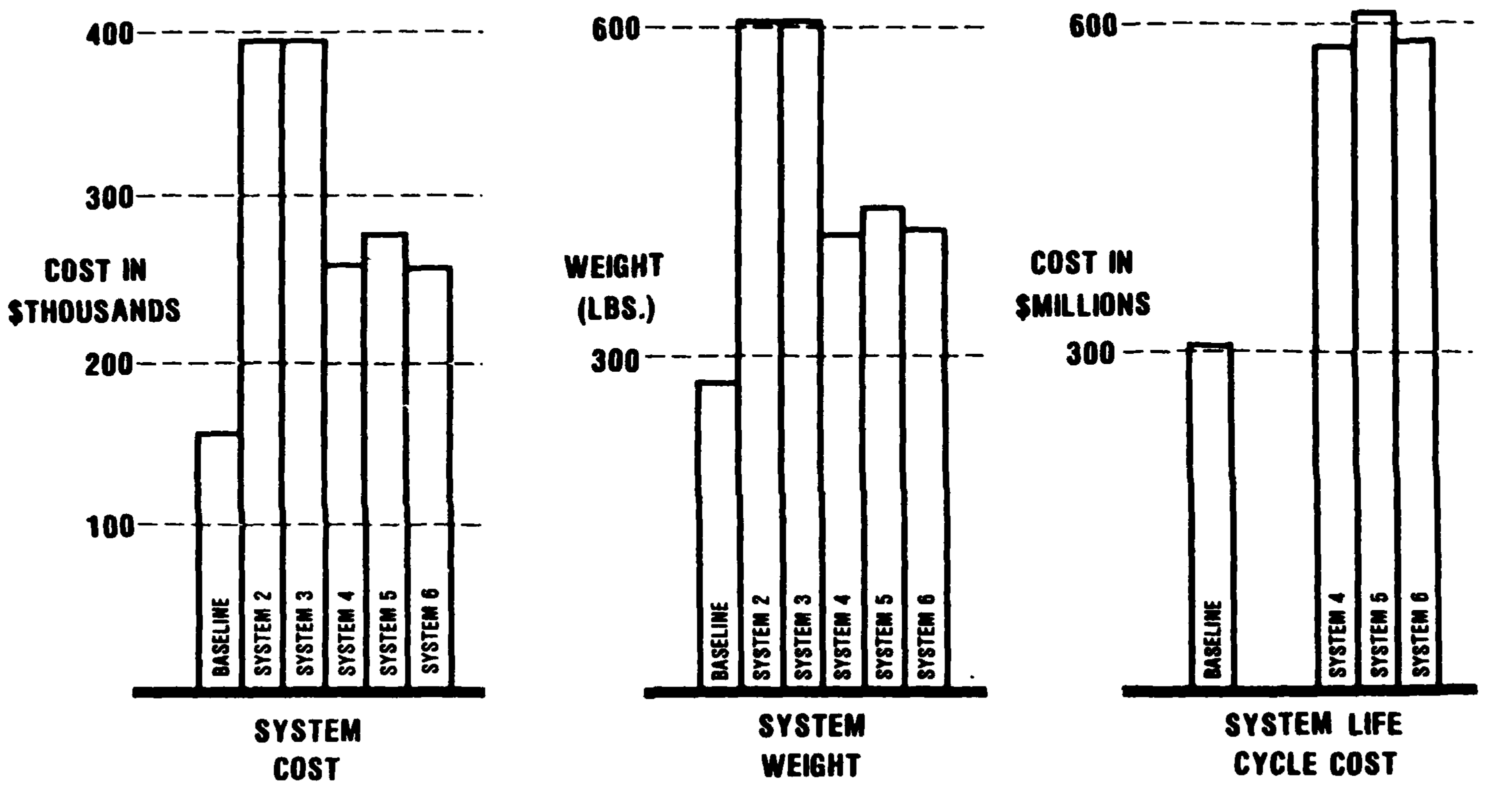


Figure 3. FAFTEEC system evaluation comparison.

SECTION III
BASELINE CONTROL SYSTEM DEFINITION

The FAFTEEC program specifically addressed the control system for the "next generation" of military combat aircraft gas turbine engines, with particular reference to Variable Cycle Engines (VCE). The GMA200 engine has been identified as the VCE under development at DDA most probable to evolve into a "future-generation" military aircraft gas turbine engine. The control system for this "future-generation" engine has been chosen as the baseline for this technology development program.

1. ENGINE CONFIGURATION

The GMA200 engine is an advanced, supersonic tactical aircraft propulsion system. Key descriptors for such an engine are single spool, variable geometry/cycle, and high-through-flow (HTF). The DDA engine concept having these features is a high temperature, variable cycle, non-augmented turbojet. Many of the key technologies a~e shown in Figure 4. The engine is applicable to tactical missions containing a high degree of sustained supersonic capability. These supersonic conditions demand the high thrust per pound of inletflow -- typical of the turbojet cycle -- and low SFC's during supersonic cruise/dash operation. The variable geometry provides the necessary flexibility to optimize thrust and fuel consumption for the various flight modes throughout the flight spectrum.

For this engine, major control system responsibilities include control of:

- o Stage fuel flow
  - Primary
  - Secondary
- o Compressor Variable Vanes
- o Turbine Variable Vanes
- o Cooling Bleed Air

HIGH TEMPERATURE, VARIABLE CYCLE TURBOJET ENGINE

APPLICATIONS: AIR SUPERIORITY FIGHTER
ATAMS

COMPRESSOR

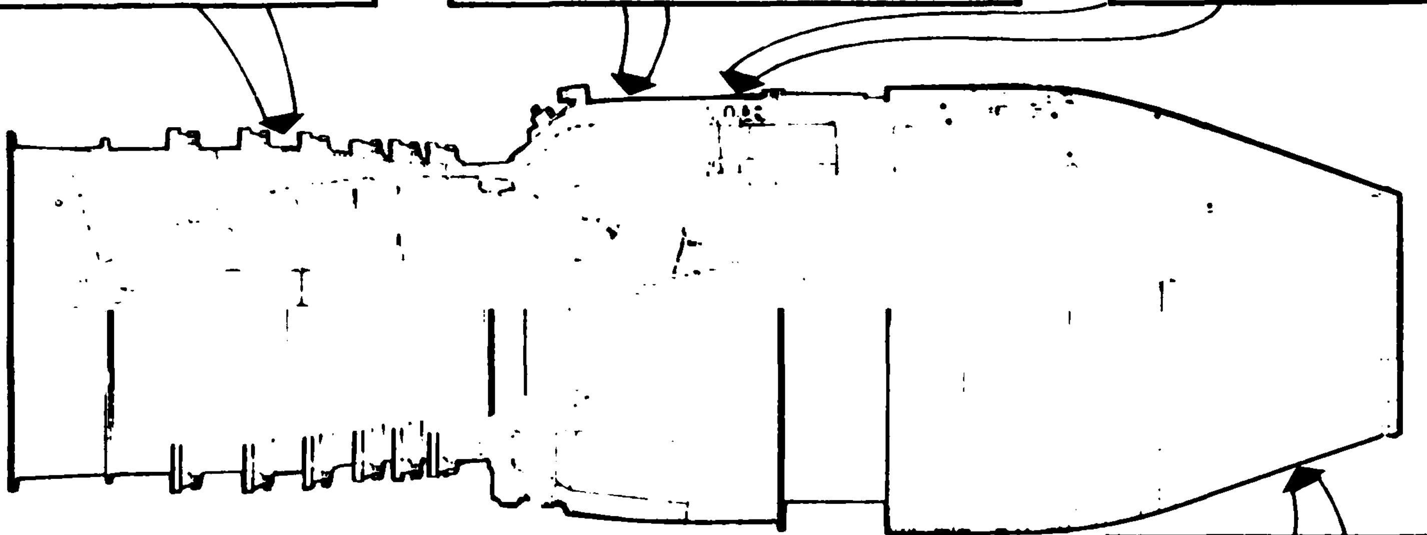
- HIGH THROUGH FLOW
- HIGH STAGE LOADING
- VARIABLE GEOMETRY VANES

DIFFUSER/COMBUSTOR

- HIGH MACH ANNULAR COMBUSTOR WITH LAMILLOY COOLING
- STAGED FUELING

TURBINE

- HIGH TEMPERATURE
- LAMILLOY COOLING
- VARIABLE VANES
- MODULATED COOLING



NOZZLE

- AXISYMMETRIC CONVERGENT

Figure 4. DDA High Temperature, Variable Cycle Turbojet Engine.

- To the Turbine Blades
- To the Aft-Section Shroud

- Exhaust Variable Nozzle

The coordinated control of these variables, as required to achieve the maximum performance for the full realm of operation, can only be practically accomplished with a full authority digital electronic control system.

2. BASELINE CONTROL SYSTEM CONFIGURATION

The baseline control system is shown as a block diagram representation in Figure 5. The system structure is basically designed to provide the required coordinated control functions without redundancy. The exception to this is the use of dual speed sensors, fuel pumps, and fuel metering systems.

The following is a brief description of each of the various control system components shown in Figure 5.

a. Digital Controller

The digital electronic controller is an engine mounted fuel cooled unit which employs advanced technology. As a baseline configuration it has no redundancy.

It consists of nine modules or major elements as indicated in Figure 5. The major elements within the controller include:

- a central processing unit (CPU)
- memory
- analog to digital (A/D) inputs circuitry
- temperature conversion circuitry
- excitation circuitry
- output circuitry
- a power conditioning circuit
- a 1553 data bus
- a configuration control unit (CCU)

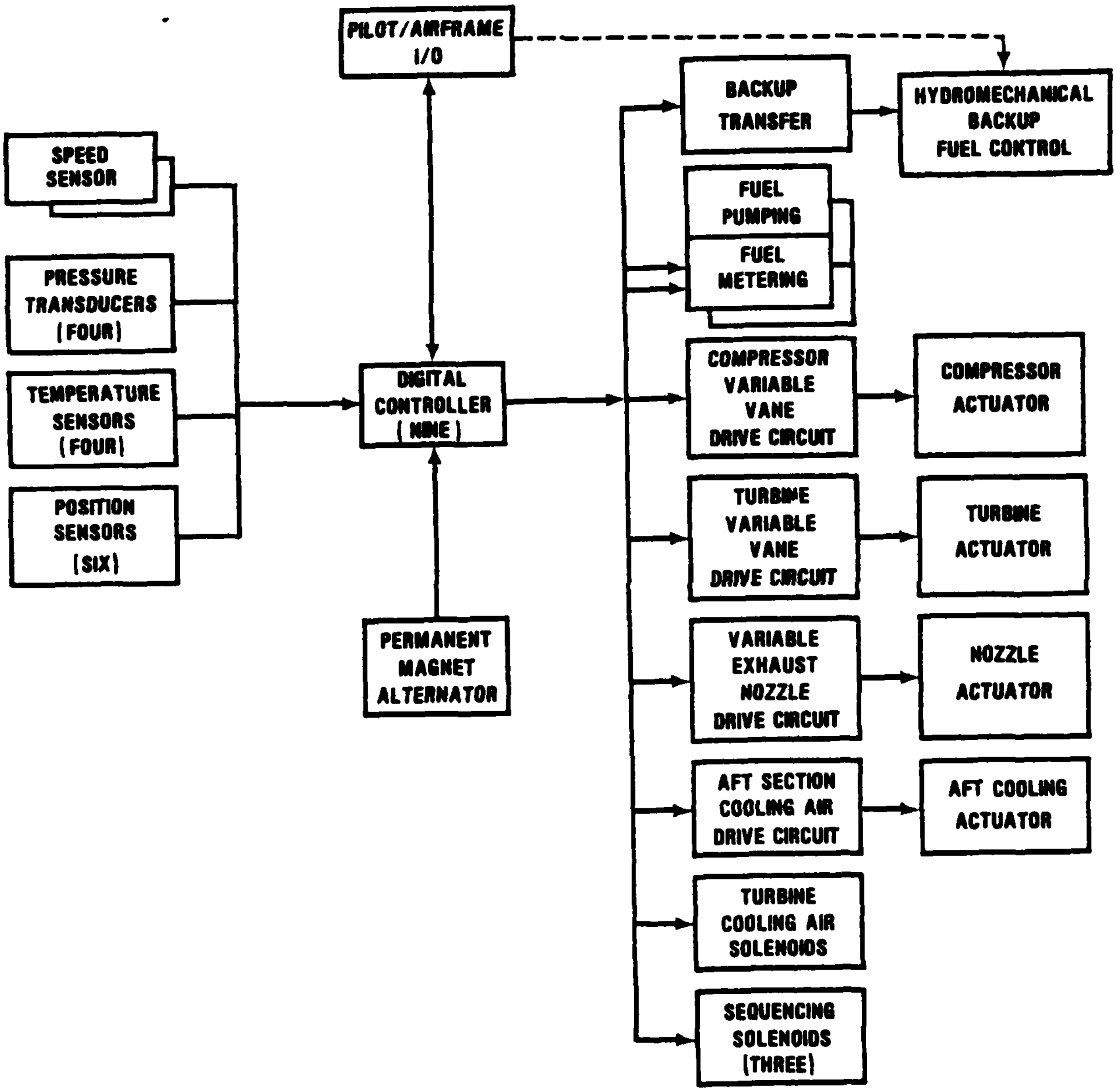

PILOT/AIRFRAME I/O
SPEED SENSOR
PRESSURE TRANSDUCERS (FOUR)
TEMPERATURE SENSORS (FOUR)
POSITION SENSORS (SIX)
DIGITAL CONTROLLER (NINE)
PERMANENT MAGNET ALTERNATOR
BACKUP TRANSFER
HYDROMECHANICAL BACKUP FUEL CONTROL
FUEL PUMPING
FUEL METERING
COMPRESSOR VARIABLE VANE DRIVE CIRCUIT
COMPRESSOR ACTUATOR
TURBINE VARIABLE VANE DRIVE CIRCUIT
TURBINE ACTUATOR
VARIABLE EXHAUST NOZZLE DRIVE CIRCUIT
NOZZLE ACTUATOR
AFT SECTION COOLING AIR DRIVE CIRCUIT
AFT COOLING ACTUATOR
TURBINE COOLING AIR SOLENOIDS
SEQUENCING SOLENOIDS (THREE)

Figure 5. FAFTEEC Baseline Control System

Some of the other modules depicted in Figure 5 actually contain components which are housed in the digital control assembly. These include the electronics portion of the pressure transducers and the torque motor drivers in the variable geometry drive circuits, among others. These have been broken apart from the digital controller so as to logically remain with the sensors and actuators.

b. Fuel System

The GMA200 combustor has two sets of fuel nozzles. The primary nozzle set operates at low power while both sets operate at mid and high power settings to achieve the desired fuel/air ratios for each nozzle set. Trade studies have shown that the GMA200 can complete its missions with only one set of nozzles operative. Therefore, the present GMA200 control system has dual pump and metering systems -- one for each nozzle set as shown in Figure 6.

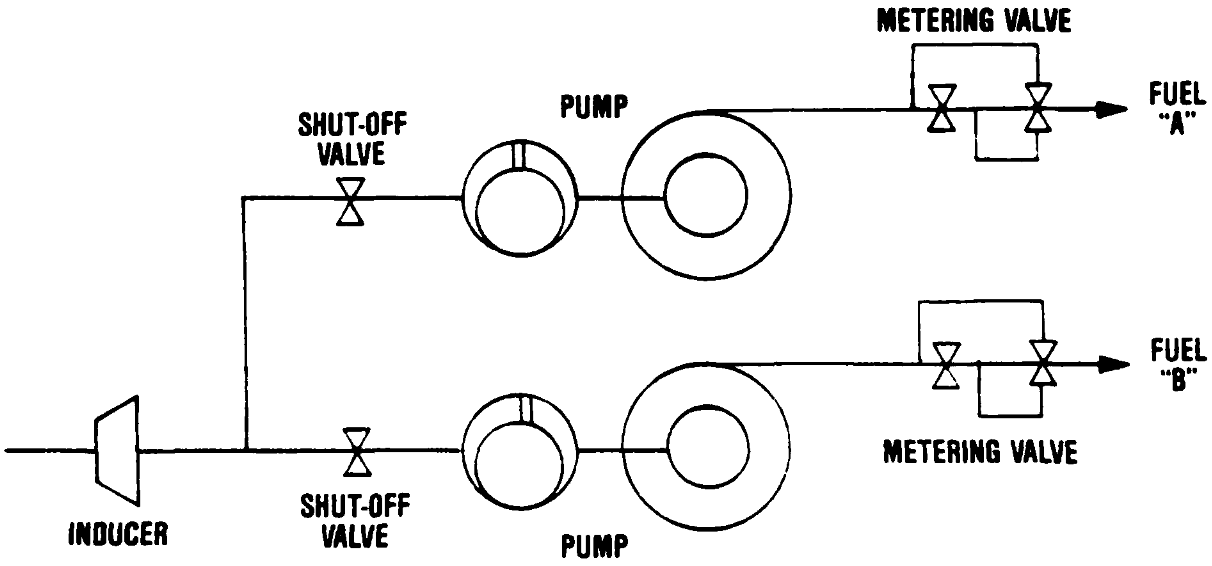


Figure 6. FAFTEEC Baseline Fuel Metering System.

Each fuel pump/control assembly consists of 1) an inducer element which keeps the main centrifugal element filled with fuel at all inlet pressure conditions, 2) a retracting vane starting pump, 3) a high pressure centrifugal impeller surrounded by a free wheeling rotating diffuser to reduce drag friction, and 4) a pressure drop type metering control.

The metering control contains a torque motor which uses a signal from the engine electronic control to operate a fuel servovalve which in turn positions a rotary fuel metering valve. The fuel metering valve controls the amount of fuel going to the engine. Downstream of the metering valve is a throttling valve whose function is to control the pressure drop across the metering valve to a fixed value. Since fuel flow is a function of metering valve area and its pressure drop, fuel flow to the engine is controlled directly by the electrical signal to the torque motor servo. Throttle valve position is determined by a spring and a regulated fuel pressure drop which is generated by a differential pressure sensor which measures pressure drop across the metering valve. A pressurizing valve is located downstream of the throttle at the control exit. Its function is to maintain a more nearly uniform gain over the flow range.

Each system also incorporates a main shut-off valve which prevents fuel contained in the pump/control assembly (control metering valve is in min. low stop setting) from passing into the combustion chamber, collecting there and causing a hot start. When the shut-off valve is closed, the main and primary fuel nozzles are purged of fuel and vented overboard via the nozzle manifolds by means of combustion chamber gas pressure. The start valve is controlled by a solenoid operated fuel servo valve which is activated open (manifold drains closed) during a start and activated closed (manifold drains open) during shutdown by a discrete signal.

c. Compressor Geometry Actuation System

GMA200 features an axial flow compressor assembly consisting of subassemblies of the rotor, the case and variable vanes, and the front bearing support and sump.

The case and vane assembly supports all stages of variable vanes. The first-stage vanes are tied together at the hub end by a segmented inner ring. The remaining variable vane stages are cantilevered from the compressor case. All stationary vane rows except the outlet guide vanes have the capability for variable setting angle. This feature promotes maximum variability in airflow capacity and a flow-speed relationship suitable for supersonic flight. It also allows surge relief at low compressor speeds.

The compressor actuation system is a fuel actuated hydraulic actuation system controlled on corrected speed by the digital controller through an Electro-Hydraulic Servo Valve (EHSV) and a vane position transducer. A pair of hydraulic cylinders actuate a bell crank system to each vane actuation ring, one per stage of variable vanes. LVDT's sense actuator travel and provide position feedback to the controller.

d. Turbine Geometry Actuation System

GMA200 features a variable-capacity single-stage turbine with mechanically variable nozzle guide vanes and transpiration-cooled airfoils. The turbine actuation system, shown in Figure 7, has a pneumatic motor which drives multiple planocentric actuators located around the periphery of the engine by means of a high speed flexible drive cable system. The acutators in turn position a synch ring which positions the variable vanes. An electrical signal from the digital controller modulates the air supply to the motor to control the synch ring rotational rate and direction. Resolvers provide position feedback to the controller.

e. Turbine Blade Cooling Actuation System

Compressor discharge air is directed onto the turbine blades by 30 individual poppet valves. These valves are held closed with compressor discharge air at a control port and activated by venting the control port to atmosphere. These control ports may be individually controlled or manifolded together.

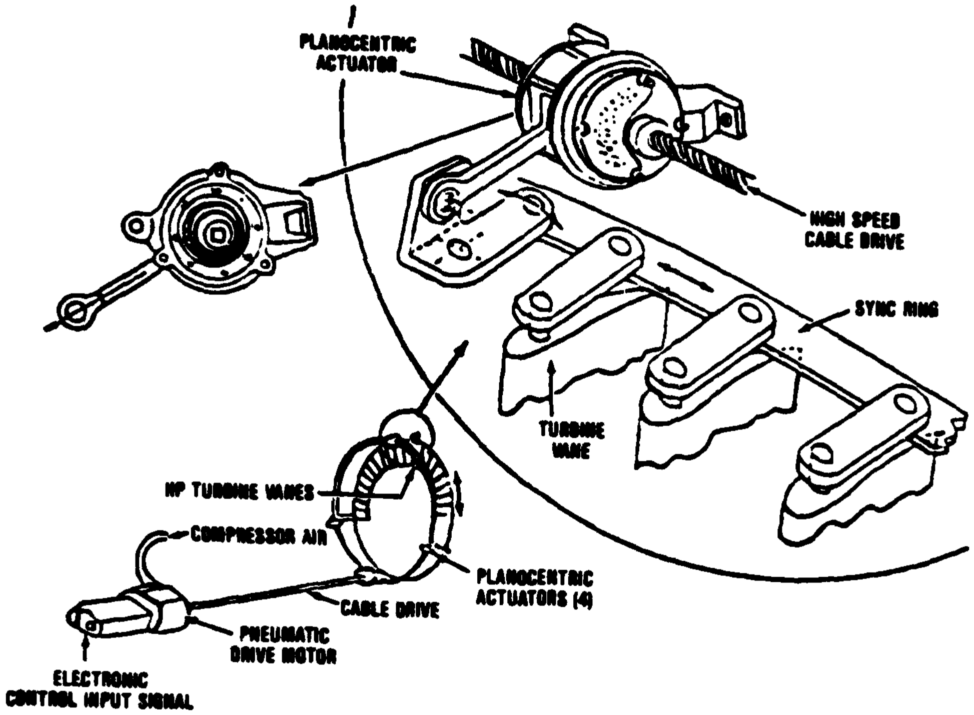


Figure 7. Turbine Actuation System.

A turbine blade cooling scheme using 4 on/off solenoid valves is shown in Figure 8. Four discrete signals are provided from the digital controller to operate the four solenoid valves. The solenoid valves are connected to manifolds W, X, Y, and Z which control 16, 8, 4, and 2 poppet valves respectively.

f. Aft Section Cooling Modulation

Cooling air to the rear support and nozzle is supplied from a compressor outer bleed. The air is transferred aft via a circumferential duct around the outside of the hot section of the engine (combustion and turbine sections).

The aft section cooling modulation actuation system consists of a ring-valve and an air motor/planocentric drive system. The planocentric drives are located in the rear support area (hot section) and the air motor in the compressor section similar to the HPT arrangement.

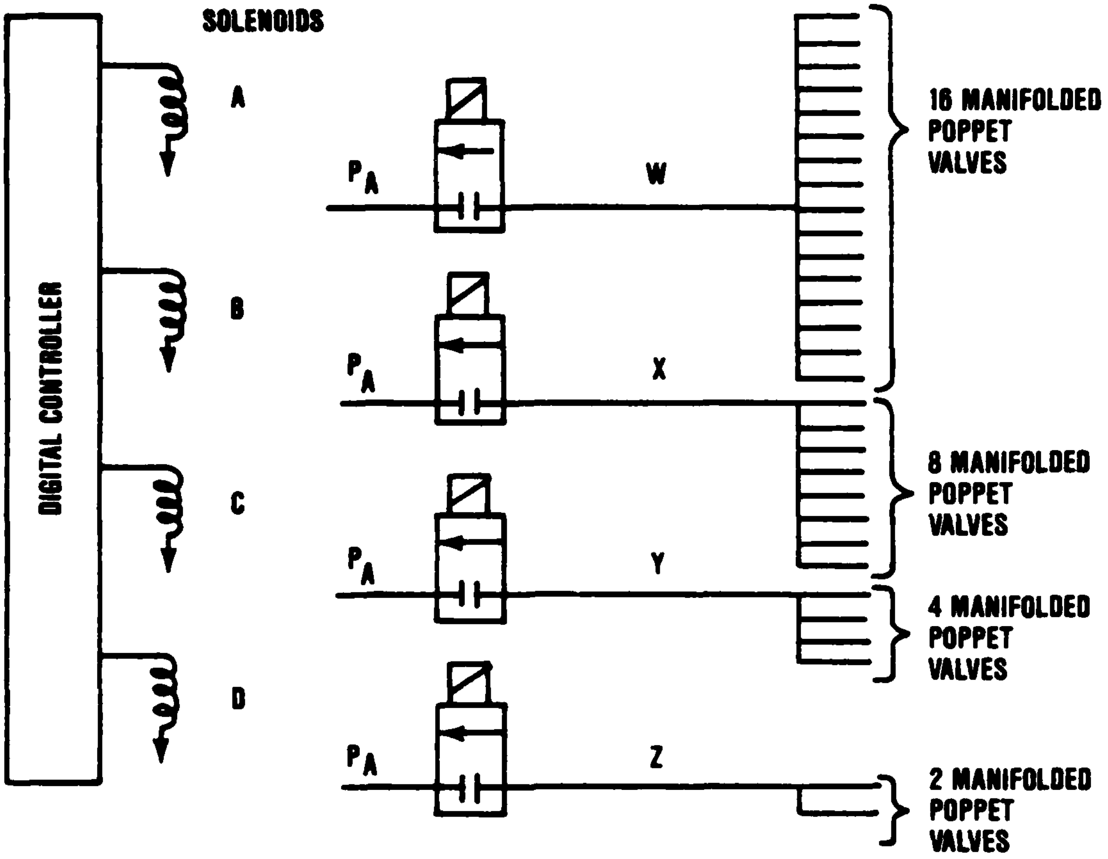

SOLENOIDS
DIGITAL CONTROLLER
A
B
C
D
P_A
P_A
P_A
P_A
W
X
Y
Z
16 MANIFOLDED POPPET VALVES
8 MANIFOLDED POPPET VALVES
4 MANIFOLDED POPPET VALVES
2 MANIFOLDED POPPET VALVES

Figure 8. Vane Cooling Modulation Solenoid Logic.

g. Exhaust Nozzle Actuation System

The nozzle actuation system consists of an airmotor drive through ball screw jacks to move a convergent variable area nozzle. This arrangement is structured such that the ball screw jacks are located in the hot section while the airmotor is located in the cooler compressor section.

Position control is effected through a torque motor interface and resolver feedback.

h. De-Ice System

A de-icing system provides compressor discharge bleed air to be used for external parts requiring anti-icing. The de-icing system is operated discretely through a solenoid interface.

i. Control Feedback

The following feedback devices for the actuators, as presented in the individual actuator system descriptions, are summarized below:

1) Fuel Flow "A" -- resolver
2) Fuel Flow "B" -- resolver
3) HPC -- LVDT
4) HPT -- resolver
5) Blade cooling -- none
6) Aft cooling -- resolver
7) Nozzle -- resolver

j. Engine Sensors

In addition to the sensors used for position feedback of the controlled variables, the digital controller is also connected to magnetic pick-ups, pressure probes and thermocouples to sense speed, pressures, and temperatures.

Chromel/alumel thermocouple clusters are used to sense temperatures at the compressor inlet and compressor discharge. Nozzle gas temperature is obtained from the output of multiple high temperature (platinum/platinum-rhodium) thermocouples. The exhaust nozzle itself is instrumented at several locations to provide a surface metal temperature to be controlled through modulation of the aft cooling.

The pressures at the compressor inlet (total and differential), compressor discharge, and nozzle are transmitted as manifolded air signals to digital Quartz transducers in the controller. These transducers produce a frequency which varies with pressure. This frequency is converted to a digital word by counter circuits.

The rotor speed is sensed through redundant channels (NHA, NHB) from magnetic pickups. The redundant channel feature allows for failure of a speed transducer to a failed-operate condition.

k. Control Input

A control input of Power Lever Angle (PLA) analagous to the desired power level shall be input to the control system. The digital controller shall receive this simplex input via the data bus.

l. Electrical System

The permanent magnetic alternator is of standard design utilizing samarium cobalt technology with multiple windings for exciters and d.c. rectified power. Multiple rectifier circuits are provided to the extent necessary to meet reliability requirements.

Dual exciters and igniters (standard practice today) are also used.

A coaxial-type wiring harness is used to electrically interface between the digital controller and all other components (previously described) in the control system. Thus multi-pin connectors on the controller interface with individual wires leading to the various sensor/effector devices through a common shielded cable.

m. Back-up Control

A hydromechanical backup control is provided in the GMA200 control system to allow fail-safe operation of the compressor variable vanes and fuel flow.

This backup control is solenoid activated via a transf?r valve. Note that the hydromechanical control is not responsible for control of the turbine or nozzle variable geometry components. Failure mechanisms associated with the turbine, the nozzle, and the bleed systems are addressed within the control mode.

3. BASELINE SYSTEM MODULAR DEFINITION

The components described in Section 2 represent the FAFTEEC Baseline Control System. In order to attack the job of improving the reliability of a system such as this, it is necessary to determine a system hierarchy and understand where these components fit into this hierarchy.

A modularization approach was used in the FAFTEEC program. Figure 9 attempts to clarify the nomenclature to be used in this modularization approach. The figure uses the components in the air motor actuation systems for illustrative purposes.

The lowest level considered with the FAFTEEC analysis was the piece part level. This refers to the items making up a control component. In Figure 9 the Pneumatic Motor Control, one of the GMA200 control components, is an assembly consisting of piece parts such as the gear motor, the vane valve, the trim spring, and others.

The component level refers to particular control system components such as the Pneumatic Motor Control, the Primary Actuator, and the Secondary Actuator. These are all separate identifiable components in the High Pressure Turbine Actuation System.

The module level represents one or more components. This is the level most commonly referred to in the FAFTEEC program. As can be seen in Figure 9, the HPT Actuator is the module in the FAFTEEC Baseline Control System representing the HPT Actuation System up to its point of attachment to the synch ring.

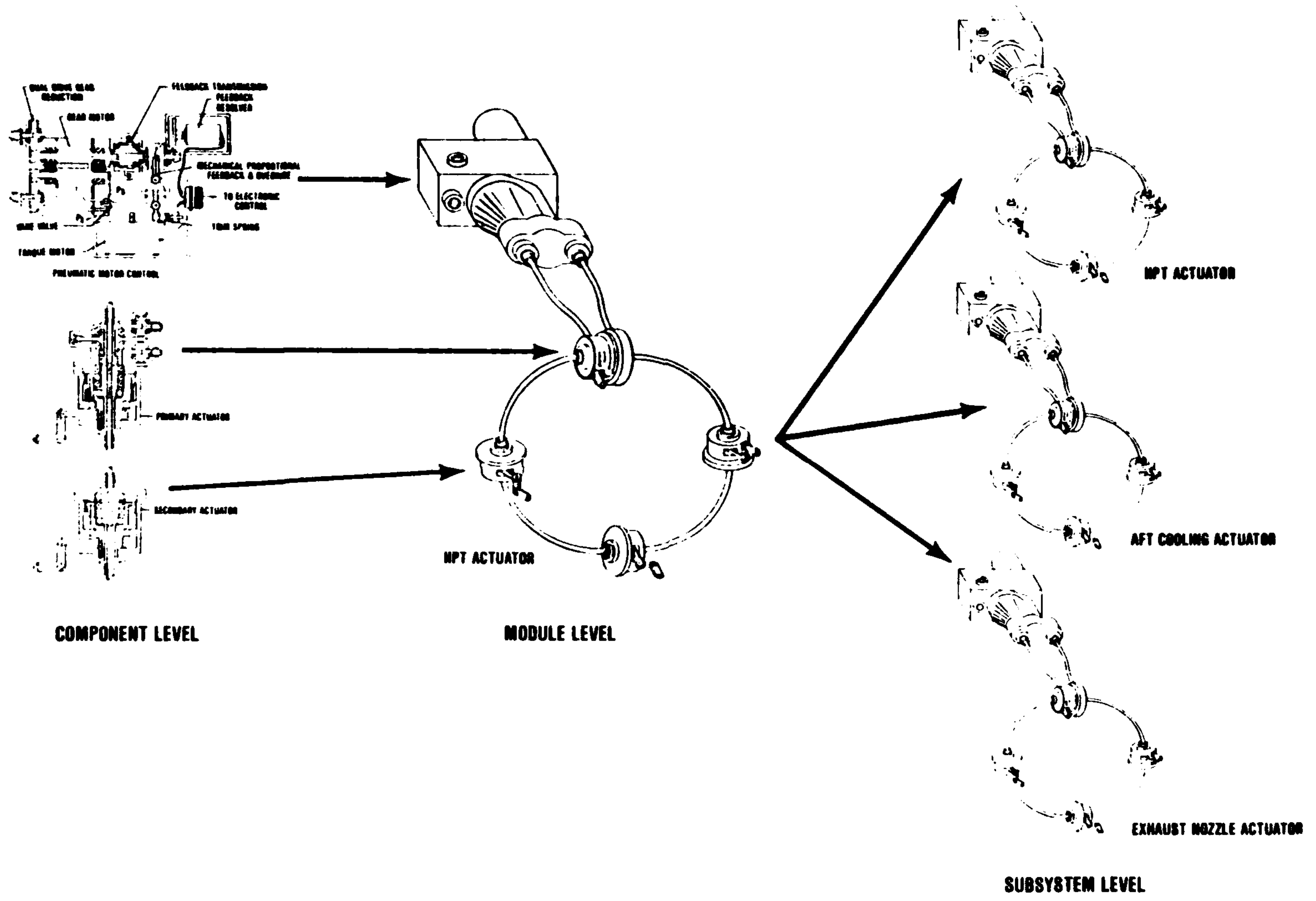


Figure 9. Modularization Approach Hierarchy

The subsystem level is a notation which implies the grouping of modules. Figure 9 shows the grouping of the three hot section actuation systems. Past the level of detail shown in Figure 9 the entire control system is comprised of multiple subsystems. In the FAFTEEC analysis the system will refer to any derivative configuration from the FAFTEEC Baseline Control System. The host will be used to refer to the engine on which the system resides.

With this terminology in mind and referring back to Figure 5, it can be noted that each solid line block represents a module of the system or a subsystem of the system where a number in parenthesis exists representing the number of similar modules in that subsystem. Layered blocks, such as those for the Speed Sensor, represent replication of modules. Thus the FAFTEEC Baseline Control System is represented by 41 modules.

Table 1 shows the block diagram designations, the FAFTEEC Baseline Control System modules corresponding to each designation, and the GMA200 Control Components corresponding to each module.

Table 1

Modular Representation of FAFTEEC Baseline Control System

Block Diagram Designation	FAFTEEC Module No.	FAFTELC Module	GMA200 Components
Digital Controller (nine)	1	Excitation	Digital Controller
	2	Databus	
	3	A/D Inputs	
	4	Temp. Common Electronics	
	5	CPU	
	6	Memory	
	7	CCU	
	8	Power Circuit	
	9	Output Module	
Fuel Metering	10	Fuel System	Metering Valve Torque Motor Dr. Shutoff Valve Solenoid Dr.
Fuel Pumping	11	Fuel Pump	Fuel Pump
Turbine Variable Vane Drive Circuit	12	HPT Drive	Torque Motor Driver
Turbine Actuator	13	HPT Actuator	Air Motor Assy.
Compressor Variable Vane Drive Circuit	14	HPC Drive	Torque Motor Driver
Compressor Actuator	15	HPC Actuator	Hyd Cylinder Assy.
Aft Section Cooling Air Drive Circuit	16	BLD2 Drive	Torque Motor Driver
Aft Section Actuator	17	BLD2 Actuator	Air Motor Assy.
Variable Exhaust Nozzle Drive Circuit	18	A8 Drive	Torque Motor Driver
Nozzle Actuator	19	A8 Actuator	Air Motor Assy
Turbine Cooling Air Solenoids	20	BLD1 Drive	Solenoids Driver
Speed Sensor	21	Speed Sensor	Pick-up Circuit
Temperature Sensors (four)	22	CIT Sensor	Harness Circuit
	23	CDT Sensor	Harness Circuit
	24	EGT Sensor	Harness Circuit
	25	TNO2 Sensor	Harness Circuit
Pressure Sensors (four)	26	CIP Sensor	Sensor Electronics
	27	Δ P Sensor	Sensor Electronics
	28	CDP Sensor	Sensor Electronics
	29	EGP Sensor	Sensor
Position Sensors (six)	30	WFA Sensor	Resolver Circuit
	31	WFB Sensor	Resolver Circuit
	32	A8 Sensor	Resolver Circuit
	33	HPT Sensor	Resolver Circuit
	34	BLD2 Sensor	Resolver Circuit
	35	HPC Sensor	LVDT Circuit
Sequencing Solenoids (three)	36	Exciter/ Igniter	Solenoid Driver
	37	Airstart	Solenoid Driver
	38	Di-Ice	Solenoid Driver
Permanent Magnet Alternator	39	PMA	PMA
Backup Transfer Value	40	BU Transfer	Solenoid Driver
Hydromechanical Backup Control	41	Hydromechanical BU Control	Hydromechanical Backup Control

SECTION IV
CONFIGURATION OF FAULT-TOLERANT SYSTEMS

The objective of the FAFTEEC prɔgram was to evolve design guidance via study and analysis with respect to one facet of the reliability/availability/integrity issue associated with the future development of digital electronic engine control systems: that of providing for very high reliability/fault-tolerance through the judicious use of redundancy, tailored to the needs of variable-cycle engine (VCE) control, and optimized with respect to the reliability of the system, of its individual elements, and to its cost-of-ownership. That is, what form(s) of redundancy and what level(s) of component reliability could lead to desired system attributes at optimal cost? The program approach was to select a typical aircraft electronic engine control system and improve its system reliability, system availability, and system fail-operational capability. The previous section described the baseline system to be used in FAFTEEC. This section focuses on the issues and concepts involved in achieving a fault-tolerant structure and the method used in configuring some candidate "fault-tolerant" systems.

1. FAULT-TOLERANT SYSTEM GOALS/CONSTRAINTS

At the beginning of this program, the Air Force Aero Propulsion Laboratory and the DDA/DE/SCT study team jointly developed a set of design goals for formulating candidate fault-tolerant system configurations. These factors represented "acceptance" criteria for proposed fault-tolerant system designs. The goals dealt explicitly with the issues of system safety and effectiveness.

a. System Effectiveness Goals

The following system effectiveness design goals were established at the inception of this program.

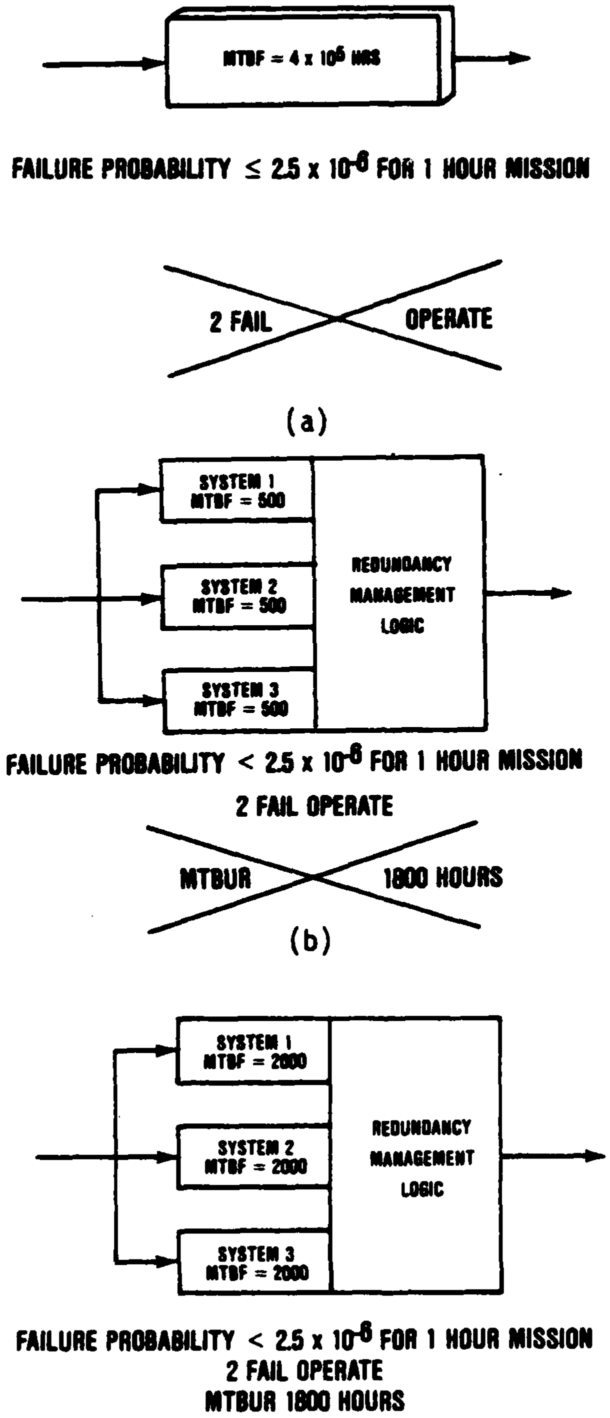
- o system failure rate $\leq 2.5 \times 10^{-6}$ failures/hour
- o 2 - fail operational capability
- o system availaɒility $\geq$ 1800 hours

Within the FAFTEEC program, system failure rate implies failure of a critical component in the control system causing the aircraft mission to be aborted. The system failure rate goal of 2.5 x 10^{-6} failures per hour can be alternately stated as 2.5 failures per million hours (FPMH). Failure rates in this report will normally be expressed in units of FPMH. Stated in another fashion, the goal for probability of successful mission completion for a particular mission was established as $\geq$ .9999975. This number represents 1 minus the system failure rate.

Fail-operational capability implies sustaining a failure of a component but, through the implementation of fault-tolerant concepts, allowing the system to remain operational to the point that the aircraft mission can be successfully completed. A 2-fail operational capabilitity, the goal used in this fault-tolerant system design study, indicates that 2 system components can fail and the system will remain operational, enabling continued safe and effective flight operation.

The system availability goal relates to mean time between unscheduled removals (MTBUR). This is an indication of operational readiness, a primary concern for military aircraft applications.

There is a strong relationship among these goals. For example, Figure 10(a) illustrates a highly reliable simplex system that meets the failure rate requirement but cannot tolerate two failures. A triplex system could clearly satisfy the 2-fail operational requirement. Figure 10(b) is an example of a configuration that satisfies both the failure rate and operational acceptance criteria, however, assuming that the triplex modules each have a mean time between failure (MTBF) of 500 hours, the system cannot satisfy the availability requirment. By increasing the MTBF to 2000 hours as shown in Figure 10(c), the availability measure can be met.



(c)

Figure 10. Relationship of System Effectiveness Issues

b. Other Goals

Although the above 3 system effectiveness issues were the primary drivers in design of fault-tolerant control systems, other less quantifiable issues impacted the fault-tolerant system designs. These issues included:

- o Failure Recovery Considerations
- o Environmental Tolerance Considerations
- o System Overhead Considerations

(1) Failure Recovery Considerations

In configuring fault-tolerant systems, there is obviously a desire to recover in a timely and efficient manner from any component failures so as not to create system failures. The efficiency involved with recovering from component failures is indicated by a parameter called coverage. The timelinesss of recovery affects recovery strategies and therefore needs to be quantified.

Coverage is one of the most critical issues in fault-tolerant system design. It is a measure of the confidence associated with the fault accommodation of the system. Stated mathematically it is the conditional probability that the system detects, isolates, and recovers operation given the occurrence of a fault.

Figure 11 is a Markov model of a system with n replicated modules. For the purpose of this analysis, if the example system accommodates the first fault, system failure occurs only if the remaining n-1 modules fail. This is represented by the two possible exit paths from the initial state, s^n. Transition probabilities are indicated for the two paths. Therefore, the probability of system failure, $P_{failure}$, is:

$$P_{failure} = n(1-c)\lambda$$

where

n = number of modules

c = coverage

λ = module failure rate (failures/hour)

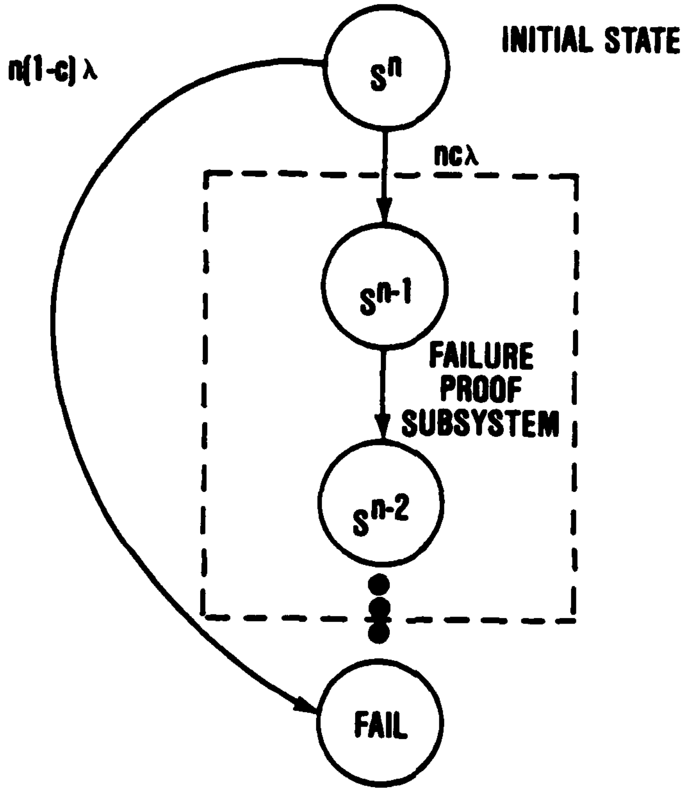


Figure 11. Markov Model Illustrating Coverage

A system failure rate ($P_{failure} \leq 2.5 \times 10^{-6}$) was established in the Section 4.1.1. The following relationship satisifies this requirement.

$$2.5 \times 10^{-6} = n(1-c)\lambda$$

Thus, a five module configuration with 500 hours MTBF ($1/\lambda$)would require coverage of .9998. A three module configuration with substantially higher MTBF (2000 hours) would need a coverage of .9988.

Failure recovery time is dependent upon the type of failure and the condition under which a failure occurs. A major criteria in the GMA200 control design process was to make failure modes as "fail-safe" as possible. That is, to the maximum extent possible, any failure should drive the system to a safe operating mode. For example, loss of a computer command would drive the affected actuator position that minimizes surge, overtemperature, overpressure or overspeed conditions. The most critical failure for the specified application was the one that would increase the fuel flow during an acceleration (e.g., failure of a feedback sensor). Failure to reduce the fuel flow at the end of an acceleration could cause thermal damage to the turbine in less than 0.25 second. Therefore, a maximum failure recovery time of 250 milliseconds was established for all fault-tolerant system designs.

(2) Environmental Tolerance Considerations

A ground rule for fault-tolerant system designs was that they shall function safely when subjected to the normal ATF operating environment or levels of lightning and EMI/RFI/EMP radiation. Since FAFTEEC does not address the detailed design of a digital controller, it was assumed that design techniques met requirements for voltage spikes and radiated energy. Furthermore, it was assumed that these phenomena affect system reliability only in the sense that system would become more complex in providing the required protection -- no failures were attributed to them.

The ATF mission definition dictated the operating environment for all fault-tolerant system designs, especially with respect to the digital controller. By defining 90% of the missions to be 3 hours in length and the remaining missions to be 10 hours in length, the operating environment for the electronic components inside the fuel cooled digital controller (T_C)was established as:

$T_C \leq$ 57°C (135°F) for 97% of time
$T_C \leq$ 77°C (171°F) for 3% of time

The mission's effect on the engine cycle affected the environmental temperature of other control components. Thus overtemperature transients were evaluated for their effect on system reliability.

Lightning creates two problems for the digital control system. The first is the high voltage spike which may find its way to the electronics. The second is a high EMI field of short duration created by the ionization. The intensity of each disturbance is a function of the strength of the lightning and the location of the strike with respect to the control. The greatest overall damage is generated by lightning that passes through the aircraft. If the aircraft is properly designed, low resistant paths through the aircraft will be provided to channel the lightning energy away from sensitive electronics. Thus, the control must void these paths and be electrically isolated from the frame in general.

Even when not struck by lightning, flying in a thunderstorm subjects the aircraft to large "cross-field" EM transients. Although these field strengths are approximately an order of magnitude less severe than a direct strike, their occurrance is several orders of magnitude greater than direct strikes. Fortunately, proper EMP and lightning direct-strike projection will eliminate any threat from "cross-field" EM transients(1). This protection consists of electronic design procedures that "filter" out large spike inputs of voltage or current. In addition, the aircraft body is designed to carry the "through lightning strikes" with very large voltages which precludes the use of the aircraft structure as a signal path. The system design and fault-tolerant system design must provide proper filtering for lightning and EMI/RFI/EMP.

The RFI is generally covered by the EMI protection and EMP protection is common with the lightning "cross-field" EM transients discussed above.

All of these are considerations which must be addressed in hardware design of fault-tolerant systems. The FAFTEEC program did not address this detailed hardware design issues but rather assumed that sound environmental protection practices had been observed.

(1) J.A. Plummer, "Analysis and Calculation of Lightning Induced Voltages in Aircraft Electrical Circuits," NASA Contractor Report CR-2349, prepared for NASA LeRC, January, 1974.

The FAFTEEC analysis does consider other environmental effects.

In the event the control system is subjected to levels beyond the protection levels, the system shall revert to a backup mode. The transfer to the hydromechanical control will be automatic upon the loss of a signal indicating system health from the digital controller.

(3) System Overhead Considerations

The impact on availability/reliability and cost and weight of all the elements of the fault-tolerant system included therein shall be included in any analysis; i.e., the use of redundancy implies the presence in the system of not only additional modules/channels, but also: Voter circuitry, line monitors, "intelligent" switches, BITE equipment, etc., sometimes termed "overhead".

It is very important that the cost of this redundancy be clearly understood and appreciated if it is to be accepted generally and used effectively. There should also be a reflection of the influence of maintenance policies and philosophies developed to specifically accommodate fault-tolerant systems.

2. FAFTEEC CONCEPTS

The issues discussed in the previous section are by-products of control system designs. Stated in another manner, they are actually the dependent variables in the control design process. The independent variables in the FAFTEEC control design process are those parameters which make the baseline system more reliable or more available or more fault-tolerant. Three general concepts were used to promote fault-tolerant system designs in FAFTEEC. They included:

- o Redundancy
- o Fault Recovery
- o Maintenance

a. Redundancy

The FAFTEEC candidate fault-tolerant control systems were constructed as variations to the baseline system with redundancy used on the digital controller, sensors, actuators, and other components to achieve a desired reliability. The approach was to use redundancy to various degrees within the digital controller, itself, as well as at the component level. Two types of redundancy, hardware replication and analytical redundancy, were used.

(1) Replication

Systems generally are constructed of several (assumed to be) independent modules, and each module has a given failure rate. For a system without module redundancy the system failure rate is computed as the sum of the module failure rates. If failure of any one module causes a system failure then that module is deemed critical. The only way to improve the reliability for such a system is to improve the individual module reliability or use more than one identical module to accomplish a critical function. This use of replication implies, for example, that one module act as prime while the other module(s) remain as back-ups to be used if the prime module fails. Thus failure of a module would not cause a system failure, provided that the back-up module is successfully brought on line.

Replication was a prime reliability improvement approach evaluated in the FAFTEEC design process.

(2) Analytical Redundnacy

Analytical redundancy methods are an alternative for resolving conflicts between cost and weight of hardware redundancy (replication) and overall system reliability requirements. These methods were applied to sensors in the FAFTEEC program.

The basic idea of analytical redundancy is to use known dynamic relationships between different sensor outputs in order to detect failures. Mechanizing these concepts ranges from using simple complementary filters to complex banks of model following filters (e.g. Kalman filters or observers). The principle of operation for each concept is the same - test whether the actual sensor outputs satisfy known functional relationship that exist between these outputs. The sensors are healthy if the relationships are satisifed; they have failed somewhere if the relationships are violated.

Analytical redundancy was used in the FAFTEEC program for redundancy with respect to noninterchangable sensors (pressures, temperatures).

(b) Fault Recovery

Given that there is a provided-for capability to improve system reliability through redundancy, there is a need to identify and recover from module failures to take advantage of this redundancy. This ability is associated with fault recovery.

Many fault recovery strategies exist. These include self test procedures, voter techniques, etc.

The fault recovery capability of a system is a measure of the fault detectability, isolatability, and recoverability. One quantitative measure of this capability is the coverage. Coverage, as previously discussed, is the probability that if a system fails in a particular state, that failure will be detected, isolated, and recovered, and operation will continue at the same or tolerably reduced level of performance.

Any fault recovery strategy applied to a given redundant system has an associated coverage value. This coverage value is the probability that any failure mechanism can be accommodated.

As an example consider a system consisting of two identical modules operating in a Standby Replacement mode (one spare maintained in an inactive mode while the other module is active). If the fault recovery method can identify and recover from 99% of the failures associated with the module, the coverage is .99.

Coverage, therefore, is another vital independent variable in the FAFTEEC design process. It should be noted that a coverage value is associated with a particular module, its redundancy level, and the fault recovery strategy used. Thus the fault recovery strategy used could well limit the coverage value attainable.

(c) Maintenance

Air Force engine maintenance policy for the 1980's has been defined using the principles of Reliability Centered Maintenance (RCM). RCM has its origins within the airline industry. Its objective is the specification of a maintenance program that "achieves the inherent safety and reliability capabilities at a minimum cost". The major policy of RCM is to eliminate the process of complete equipment overhaul. Under the overhaul concept, whenever a repairable asset, such as an engine, attains a designated maximum operating age, it is removed and transferred to a depot facility for complete teardown, inspection, component replacement and reassembling in accordance with standard technical orders. When the engine is returned to service the operating age is reset to zero on the assumption that the overhaul has returned the asset to a state comparable to its original condition. The major problem with complete overhaul is the ever increasing cost (manpower, resources, etc.) it incurs in maintenance related events. The continued policy of complete engine overhaul alone has been shown to be a criticl cost burden to the Air Force.

Under RCM, certain components are identified to have hard time limits measured in either hours or cycle counts. Scheduled engine removals are driven by the age of these components. These components are identified to be both critical to operating safety and impossible/impractical to observe for reduced resistance to failure (e.g. degradation/wear/out). The limits are established via failure mode analysis and advanced mission testing. On condition maintenance (OCM) refers to the specification of the maintenance necessary to return a filed asset to an acceptable operational level. Under OCM, repairs are made only as required by the identifiable fault. Opportunistic maintenance (e.g. replacement of components approaching hard time limits) is prescribed to produce a cost effective maintenance action during ongoing repair. Effective application of OCM and elimination of overhaul requires the establishment of inspection and monitoring procedures to identify incipient failures and policies and procedures for redundant components.

Recent Air Force policy has dictated the management of future generations of engines and accessories as modular items. The ultimate goals of this policy are to increase engine availability and minimize downtime. This is accomplished by isolation of engine and accessory faults to the modular level. The failed module is replaced with a spare from inventory and the engine is reinstalled in the aircraft. Depending on level of repair, parts availability, and work load, the module is repaired locally or transported to the depot.

A mix of OCM and RCM was used in the FAFTEEC design process. RCM requires identification of mission critical/safety critical components with hard time limits (e.g. cables, fuel valve). Fault recovery capabilities will play a key role in the identification and specification of maintenance. The capabilities would be required to provide trained personnel with the tools/ techniques to group recoverable system failures into categories requiring critical maintenance, and deferred maintenance. Critical maintenance would dictate that the controls be immediately removed and transferred to an intermediate maintenance facility for repair. Deferred maintenance designates items for which maintenance could be delayed without compromising the operational integrity of the system. For example, the decision to replace an analytically redundant sensor internal to the engine could be delayed until the engine was removed for repair.

Opportunistic maintenance would apply when the system has been removed for repair in connection with engine removals. Thus a non-control related maintenance action provides an opportunity for maintenance on the control. It is the determination of what additional refurbishment, inspections, and component replacements would be applicable and cost effective.

The proposed design for a fault-tolerant system in this program is essentially modular in nature The requirement to maintain the equipment modularly at the intermediate maintenance level implies that personnel would be provided with tools for fault isolation to the board level and that "sufficient" spare modules be stocked at base. The explicit details of these procedures cannot be implemented without optimum repair level analysis (ORLA). Aspects of the ORLA principles (cost, repair level, support, etc.) were incorporated into the detailed simulation.

The overriding issue evident in the development of FAFTEEC's maintenance strategy is that it is inexorably tied to engine mission, operations, and support. The digital electronic control will operate in the single/dual engine tactical fighter environment. These engines routinely experience a mean time between removal on the order of 160 hours. Whenever the engine is removed, an opportunity exists to perform a preventative maintenance action on the controls. This maintenance opporunity impacts the decision to defer non-critical fault-tolerant system maintenance as well. This relationship between the engine (higher assembly) and the fault-tolerant control system was factored into the evaluation in the simulation.

3. TECHNOLOGY TRANSFER

During the FAFTEEC program utilization was made of work done by researchers outside the engine development community with fault-tolerant digital computer-based systems. These technology sources came from the communications industry and the automotive electronics control community. As the technology sources from the communications industry, Bell Telephone Laboratories (BTL) was chosen because of their position as a leader in both fault-tolerant computing and electronic device reliability. The automotive community was represented by the Delco Electronics Division of the General Motors Corporation due to its recent introduction of large numbers of autmotive electronic engine controllers into production.

The objective of the Technology Transfer was to identify critical redundant system constraints and to evaluate these constraints with respect to existing designs. Ten representative fault-tolerant systems were studied for their applicability to FAFTEEC. A similar evaluation was made for an automotive engine controller designed by Delco. Finally, a detailed evaluation was made for both Delco automotive and BTL Electronic Switching System (ESS) reliability improvement techniques for semiconductor devices.

The Technology Transfer process exerted an important influence on the FAFTEEC digital controller design (see Appendix A). This controller architecture was used for all fault-tolerant designs considered during the FAFTEEC program.

(a) Redundant System Constraints

The design of a fault-tolerant computer requires that a number of constraints be taken into account, in addition to those considered in the design of a nonredundant system. The following set of design constraints was chosen to evaluate existing fault-tolerant system designs for application to FAFTEEC.

- Recovery Strategy
- Error Confinement
- Allowable Reconfiguration Time
- Coverage
- Switch Reliability
- Checker Faults
- Latent Faults
- Intermittent Faults

Recovery strategy is a fundamental system design parameter. It can vary from simple fault masking to a complicated combination of hardware/software detection, isolation and reconfiguration. Allowable reconfiguration time is closely associated with the system reconfiguration strategy. In fact it is the primary driving function in the selection of a recovery strategy. For FAFTEEC it is necessary to consider only those recovery strategies which can provide recovery times less than the required maximum of 250 milliseconds.

Error confinement to a particular module or assembly is required to validate fault independence generally assumed for reliability models. With respect to FAFTEEC, it is essential that critical system functions be maintained in the presence of two independent faults. Techniques for error confinement may be both logical and electrical. Logical error confinement is achieved through the organization of the fault reporting system. Electrical confinement is achieved at interfaces by using isolating devices such as transformers and optical isolators.

Coverage is the conditional probability that, given the existence of a failure in the operational system, the system is able to recover and continue information processing with no permanent loss of essential information. In a triplication scheme which employs fault masking, coverage is generally taken to be unity. For schemes using replication and switching, unity coverage is a desirable design goal which can be approached closely only with careful system design.

Classical replacement system reliability is limited by switch reliability. It has been shown[2] that when the reliability of the switching mechanism is taken into account, the reliability of a system with spares is not necessarily more reliable than a system without spares.

[2] Ira Terris, "Some Aspects of the Design of Self-Repairing Digital Computers," presented at the Workshop on the Organization of Reliable Automota, Pacific Palisades, California, February, 1966.

Checker faults fall into much the same category as switch reliability, with respect to their effect on system reliability. In a redundant system relying on the detection of faults with a hardware or software checking mechanism, reliability of the checker must be incorporated into the system reliability model. It is desirable that a method of checking the checker be devised such that a checker fault is not attributed to the function being checked.

A practical consideration in redundant systems is the presence of latent faults in a presumed good unit. Reliability models may be based on unity probability that all hardware is initialy fault free. In a replacement system the delays encountered in switching to a presumed good unit which turns out to be bad complicate recovery hardware or software.

Intermittent faults are one of the most difficult system constraints to account for in fault-tolerant system design. If an intermittent fault occurs once, it may be classed as a transient with a suitable procedure provided for system recovery. On the other hand, intermittents which become permanent are faults usually provided for in the fault-tolerant system. In between these extremes is the true intermittent fault, which recurs at an undefined rate.

(b) Evaluated Systems

I⁻ order to reduce the analysis of a number of technology transfer systems to a manageable task, the above set of redundant system design constraints was chosen. The task then became the evaluation of the candidate systems' ability to meet these constraints, with an eye to developing design guidelines for future systems. The choice of systems for analysis was made on the basis of technical significance, viability of the approach, and documented experience. Ten systems were chosen. Those that fall into the category of historical importance are the SATURN V guidance computer, JPL's Self Testing and Repairing (STAR) computer, and the Bell Telephone Laboratories Electronic Switching System (ESS). ESS is also the principal member of the class having documented experience, since the first ESS was put into service in the mid 1960's

Raytheon's Fault-Tolerant Spaceborne Computer (FTSC) and JPL's SCCM are outgrowths of the JPL STAR tradition. A FTSC brassboard has been completed. The MIT Fault-Tolerant Multi-Processor (FTMP) has been in development for a number of years. The Space Shuttle avionics computer uses four standard IBM AP101 computers. It is being used along with the Inertial Upper Stage (IUS) guidance computer in the Space Shuttle program. The Stanford Research Institute Software Implemented Fault-Tolerant (SIFT) computer bears careful analysis because of its software organization. The Reliability Advancement for Electronic Engine Controllers (RAEEC) Study is close in application to the FAFTEEC.

The ten systems analyzed are listed in Table 2 along with the system property which most closely characterizes each one. These characterizations are somewhat arbitrary, since there is considerable overlap of techniques between systems. For example, the Saturn V guidance computer, while classified as a TMR system, also has a duplex memory subsystem. On the other hand, the STAR standby replacment system contains a hybrid TMR test and repair processor. Many of the systems have Hamming error correcting memories, an important characteristic not listed in the table. The three systems classified as hybrid TMR are very different. One is a multi-processor, one is composed of an aggregate of standard uniprocessors, and the third is TMR structured entirely in software. Of the systems classified as duplex, only the ESS systems are on-line repairable. The IUS is a closed duplex system using standard CPU's, with special purpose hardware to enhance the fault-tolerant properites.

(c) Fault-Tolerant System Techniques Applicable to FAFTEEC

A summary of the analysis of the candidate systems for application to FAFTEEC is given in Table 2. In general, the method of satisfying the various design constraints is contingent on the exact system configuration chosen. In turn, the choice of system configuration depends on the method of satisfying the design constraints so that an iterative system design approach which includes mathematical modeling is required to achieve a quasi optimum system design.

	SATURN V (TMR)	STAR (STBY REPL)	FTSC (STBY REPL)	SCCM (STBY REPL)
RECOVERY STRATEGY	Implicit in triplication	TARP control switching of replicas.	o CCU TMR under prog. control. o When faults cannot be diagnosed, all modules powered down and brought up one at a time.	o Replace module, reload spare memory, restart program. o Executive is duplicated and cross checked.
ERROR CONFINEMENT	Error indicators associated with specific sets of voters.	o Checkers placed at buses for confinement. o Power switching, unpowered units appear as logic 0 thru isolating circuitry.	Self checking modules.	Self Checking modules.
RECONFIGURA-TION TIME	Essentially instantaneous.	Dependent on recovery program and rollback.	Dependent on recovery program and rollback.	Program dependent.
COVERAGE	Essentially unity.	Limited by "hardcore" detection circuity.	Limited by "hardcore" detection circuity.	Design goal of unity.
SWITCH RELIABILITY	Voters triplicated for protection.	Replicated buses.	Replicated buses.	Replicated buses.
CHECKER FAULTS	Disagreement detector not protected.	Detection circuits in the "hardcore".	Detection circuits in the "hardcore".	"Morphic Boolean functions" guarantee detection of checker faults.
LATENT FAULTS	Checked before launch. o Buses tested when switched in.	Standby units assumed good until fault detected.	o Standby units assumed good.	Detection by self check on-line.
INTERMIT-TENT FAULTS	Accounted for in the hardware structure.	Transient protection by repetition.	Rollback transient protection.	Application dependent.
COMMENTS	o Easy design methodology. o Uses duplex memories. o TMR section has R = 0.9986 for 250 hours.	o TARP is hybrid TMR.	o R = 0.95, 5-7 years. o Memory has Hamming code with module replacement in addition to bit plane switching. o Application program has roll-back points. o All info. data and addresses protected by codes except CPU. o CPUs are hybrid/duplex. o Faults interrupt microprogram. o 20 CMOS LSI types.	o Applied to several system configurations. o 4 Special LSI types. o Distributed computer network via MIL-STD-1553A bus. o Each computer receives commands from 1 other. o Minimization of interrupts. o Hamming code in memory.

Table 2 Analysis of Fault Tolerant Systems
(See Document 15898)

SCCM (STBY REPL)	FTMP (HYBRID TMR)	SPACE SHUTTLE (HYBRID TMR)	SIFT (HYBRID TMR)	EARLY ESS (DUPLEX)	
• Replace module, reload spare memory, restart program. • Executive is duplicated and cross checked.	Triplicated hardware at processor and memory level.	• 4 programmed minicomputers during critical phases. • After 2 failures, remaining 2 computers use self-test to provide tolerance to 3rd fault.	Software errors reported to global executive. Local exec. controls reconfiguration.	• Synchronous matched mode. • Interrupt on no match, fault recog. program, run diagnostics off-line.	Interrup switch t
Self Checking modules.	Redundant bus isolation gates limit fault propagation.	A design goal.	Write protect for other processors' memory.	Dependent on programming.	Self che isolation
Program dependent.	Depends on damage, must complete current job step (max on the order of 1 second).	Fast for 1st 2 failures. Depends on self-test execution time for 3rd failure.	Software dependent.	Depends on fault recog. program.	Maximum reload.
Design goal of unity.	Limited by hardcore detection circuitry.	Good for first two failures.	Executive software has redundant execution with majority voting.	Unity design goal.	Design go
Replicated buses.	Buses are replicated. Voting and switching hardware is distributed.	Crew interaction enhances.	Buses replicated.	Buses replicated.	Buses are
"Morphic boolean functions" guarantee detection of checker faults.	Bus guardians are duplicated.	Depends on self-test programs.	Checking is in software.	Software.	Totally u & checkers
Detection by self check on-line.	Standby spares are cycled.	Method not specified.	Could be checked by software.	Standby units are monitored.	Off-line periodical
Application dependent.	A demerit system is established to identify the most likely intermittent cause.	Crew can restart failed computer during passive orbit.	Some protection from transients because of loose synchronization.	Logged for analysis.	Elusive fa for later
• Applied to several system configurations. • 4 Special LSI types. • Distributed computer network via MIL-STD-1553A bus. • Each computer receives commands from 1 other. • Minimization of interrupts. • Hamming code in memory.	• Each processor has own cache. • Common memory among processors. • Tight sync with a fault tolerant clock. • Programmer sees as a simplex system.	• Use 5 standard AP101's. • Uses voting effectors. • Boost, reentry and landing uses 3/4 and 2/4 voting. When only 2 computers remain, self-test is the detection and isolation method. • Safety of flight effectors and sensors are internally redundant. • Voting effectors (aerosurface actuator) has 4 element, force summed actuator. Failure of any 3 of 4 channels can be tolerated. • In the duplex mode, BITE, self-test, and watchdog timer are used.	• Loose sync (up to 50 micro seconds skew) between processors. • Simply periodic scheduling. • Bendix Micro I Processor. • I/O 8080 based.	No. 1 ESS Hamming error correction. Matchers in each unit, 24 bits each @ 5.5 microseconds. No. 2 ESS No Hamming codes. Single matcher in maintenance center, matches call store input register. Matcher not used as diagnostic tool. No. 1A ESS No Hamming codes. 24 bits matched every 700 nanoseconds, 16 groups selectable. Matching used for maintenance. Memory blocks of 64K reloaded from disk for recov. Processor configuration circuit checks various times.	• No Hamm • No match • Micropro • Machine • Both sto and up lo • Maintenan force sy • Data mani duplicate

Table 2 Analysis of Fault Tolerant Systems

2

lysis of Fault Tolerant Systems
See Document 1589B)

SPACE SHUTTLE (HYBRID TMR)	SIFT (HYBRID TMR)	EARLY ESS (DUPLEX)	NO. 1A ESS (DUPLEX)	IUS (DUPLEX)	[illegible] (DUPLEX)
rogrammed minicomputers ing critical phases. r 2 failures, remaining 2 uters use self-test to ide tolerance to 3rd fault.	Software errors reported to global executive. Local exec. controls reconfiguration.	• Synchronous matched mode. • Interrupt on no match, fault recog. program, run diagnostics off-line.	Interrupt on self-check fail and switch to replacement.	Cross strap 2 computers with self-test for diagnosis.	Duplex hardware is augmented by software synthesis to achieve TMR for some functions. Recovery under software control when a BIT fail occurs.
gn goal.	Write protect for other processors' memory.	Dependent on programming.	Self checking logic and circuit isolation devices.	Serial communication link tends to isolate.	Serial communication link tends to isolate.
or 1st 2 failures. Depends f-test execution time for ilure.	Software dependent.	Depends on fault recog. program.	Maximum dependent on main memory reload. 1-2 seconds.	Limited by self-test.	Limited by program.
r first two failures.	Executive software has redundant execution with majority voting.	Unity design goal.	Design goal is unity.	Design goal 0.99.	Several "functional coverages" are used.
nteraction enhances.	Buses replicated.	Buses replicated.	Buses are duplicated.	Limited by computer communication link.	Preliminary design showed device switches to be vulnerable.
s on self-test programs.	Checking is in software.	Software.	Totally self-checking M out of N checkers.	Uses computer self-test.	Checking in software.
not specified.	Could be checked by software.	Standby units are monitored.	Off-line processor is run periodically.	Self-test runs in background.	Reasonableness checks are run to BIT.
n restart failed computer pessive orbit.	Some protection from transients because of loose synchronization.	Logged for analysis.	Elusive intermittents logged for later manual analysis.	Method not specified.	Method not specified.
standard AP101's. voting effectors. , reentry and landing uses nd 2/4 voting. When only 2 ters remain, self-test is etection and isolation d. y of flight effectors and rs are internally redundant. g effectors (aerosurface tor) has 4 element, force d actuator. Failure of any 4 channels can be tolerated. o duplex mode, BITE, self- and watchdog timer are	• Loose sync (up to 50 micro seconds skew) between processors. • Simply periodic scheduling. • Bendix Micro 1 Processor. • I/O 8080 based.	No. 1 ESS Hamming error correction. Matchers in each unit, 24 bits each @ 5.5 microseconds. No. 2 ESS No Hamming codes. Single matcher in maintenance center, matches call store input register. Matcher not used as diagnostic tool. No. 1A ESS No Hamming codes. 24 bits matched every 700 nanoseconds, 16 groups selectable. Matching used for maintenance. Memory blocks of 64K reloaded from disk for recov. Processor configuration circuit checks various times.	• No Hamming codes. • No matching (self checking). • Microprogrammed. • Machine cycle 150 nanoseconds. • Both stores are always on-line and up to date. • Maintenance personnel can force system configuration. • Data manipulation logic is duplicated.	Uses Hamming code in memory.	BIT Functions Input range Parameter correlation Parameter majority check ROM is check summed Watchdog timer Wrap around tests Injected input Canned output Reference signals Power supply test Preset scratch pad word End of conversion Several link parity Clock loss

(of Fault Tolerant Systems

3

Nevertheless, certain guidelines can be established for the choice of FAFTEEC fault-tolerant design which are configuration independent. These guidelines are summarized below in Table 3. Table 3 is a direct transfer to those system properties of Table 2 which are applicable to FAFTEEC.

Table 3. FAFTEEC Design Guidelines

DESIGN CONSTRAINT	RECOMMENDED FOR FAFTEEC
Recovery Strategy	Crew should have configuration veto power in addition to status.
Error Confinement	Use isolation devices: optical isolators, transformers, fuses, etc. Use write protect for private processor memories. Use serial communication among processors. For a replacement type system, use power switching.
Reconfiguration Time	250 millisecond maximum.
Coverage	Unity design goal for single/multiple faults.
Switch Reliability	Wherever possible, use replicated buses.
Checker Faults	Use self-checking checker hardware designs.
Latent Faults	Where the system configuration requires comparison, replacement elements should be checked periodically.
Intermittent Faults	A strategy for transient and solid faults should be devised.

A technique which appears in a majority of the systems analyzed is the use of Hamming error correcting codes in random access memories. This technique may be used for single bit per word correction at a hardware penalty of 20 to 30 percent. Owing to the speed of current semiconductor memories, it is possible to optimize the Hamming code design such that no loss of computing speed is apparent. Hamming correction is necessary for soft error correction.

For CPU error detection in a standby redundancy configuration, using a pair of microprocessors as a replacement element which is replaced when their outputs fail to compare is a viable technique. This is the approach being followed by JPL in the SCCM. As microprocessor costs come down, it seems to be the preferred approach for a small system such as FAFTEEC.

Protection of common circuits such as clocks and power supplies by redundancy is strongly recommended. Whether the system configuration requires tight or loose synchronization makes the design of redundant clocking schemes relatively difficult or easy.

The experience with ESS seems to indicate that development and maintenance cost are reduced if redundancy is cast in hardware rather than software. The use of a totally self-checking microprogram based design is recommended. The microinstruction format should be straightforward wih minimum cross-coupling between control fields.

Actuators should not be protected by replacement switching. Rather, built-in redundancy such as cited for the Space Shuttle aerosurfaces should be used. With this technique, the loss of electrical signals is fail-safe.

To minimize development costs, standard electronic part types should be used wherever possible. In the JPL-SCCM, a preliminary design indicates that only four special LSI parts be developed if existing standard parts are fully utilized. Interfacing to the crew panel via a MIL-STD-1553A bus should be considered, since this semms to be a well established standard.

Wherever possible, crew procedures should be minimized, although the decision to go to the final back-up system should be left to the crew. Status information should be made available to the crew as well.

Self-test procedures includ'̇:g built-in test (BIT) as used in RAEEC are to be highly recommended. However, some reasonableness checks may be eliminated, depending on the ultimate choice of system configuration.

4. FAULT TOLERANT SYSTEM CONFIGURATIONS

Following the design guidelines for system effectiveness and using the general concepts discussed in Section 3 (with particular attention paid to Technology Transfer Recommendations), candidate "fault-tolerant" systems were configured for reliability evaluations. These systems were all derivatives of the Baseline System.

In the Baseline FAFTEEC system block design replication of a module was depicted by a layered block. Even for the Baseline system replication was utilized for the Speed Sensor, Fuel Pumping, and Fuel Metering modules. This was done, as mentioned in Section III, for flight safety reasons. To better understand the system configuration process, Figure 5 can be redrawn as shown in Figure 12. The differences between the two figures are:

- o the nine modules in the digital controller have been shown separately in Figure 12
- o coverage value, (COV) and module maintenance policies (l) have been shown in Figure 12 for the redundant modules ($\ell = 1$ indicates repair is necessary after 1 module failure)

Figure 13 represents a derivative from the Baseline system. Note that for this given system each functional module must be defined with respect to its:

- o redundancy level
- o coverage for redundant modules
- o mainteance level

With respect to redundancy level a 2 layer block, such as for the speed sensor, indicates a duplex configuration. Similarly a three layer block repre-

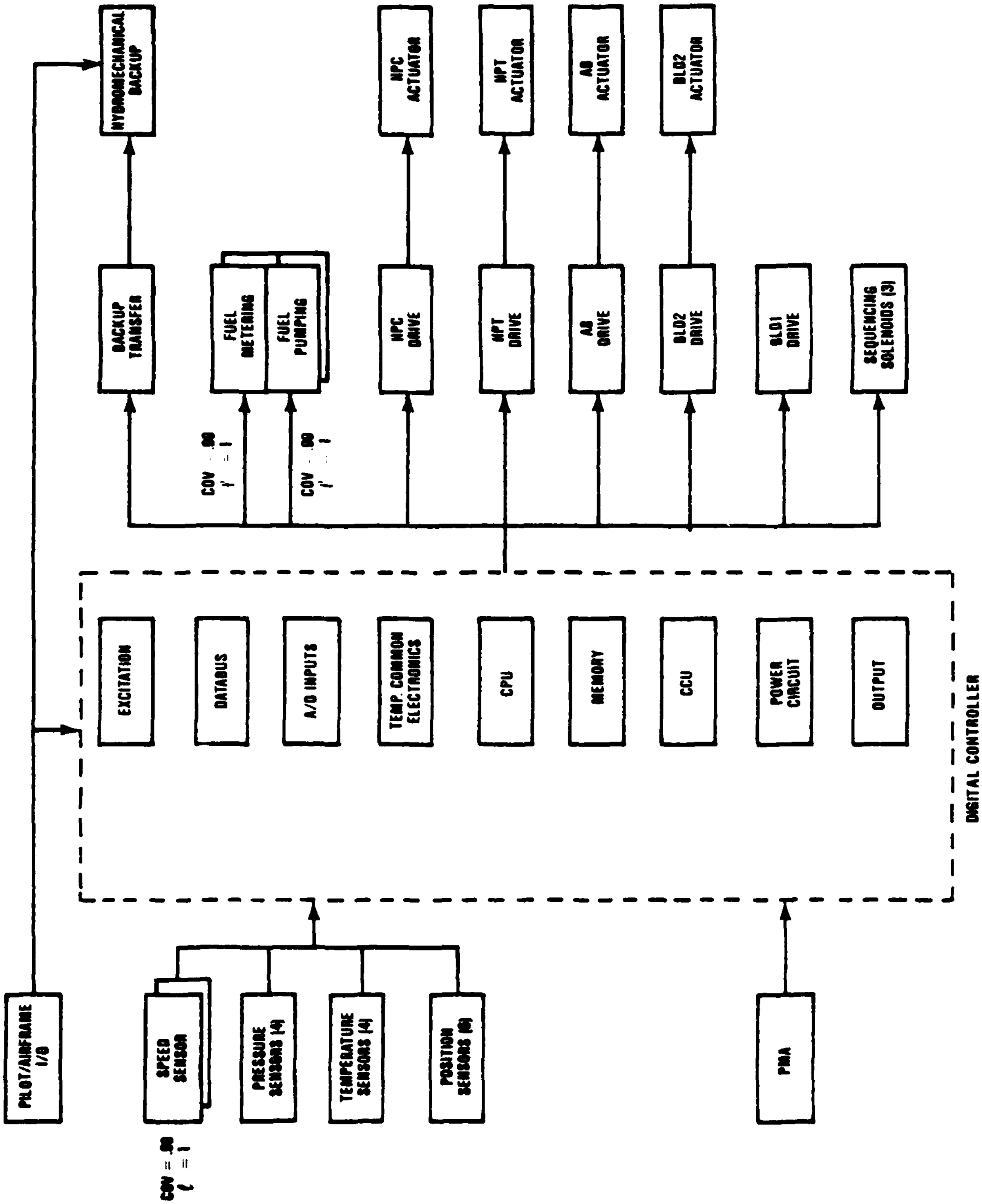


Figure 12. FAFTEEC Baseline Control System (Expanded)

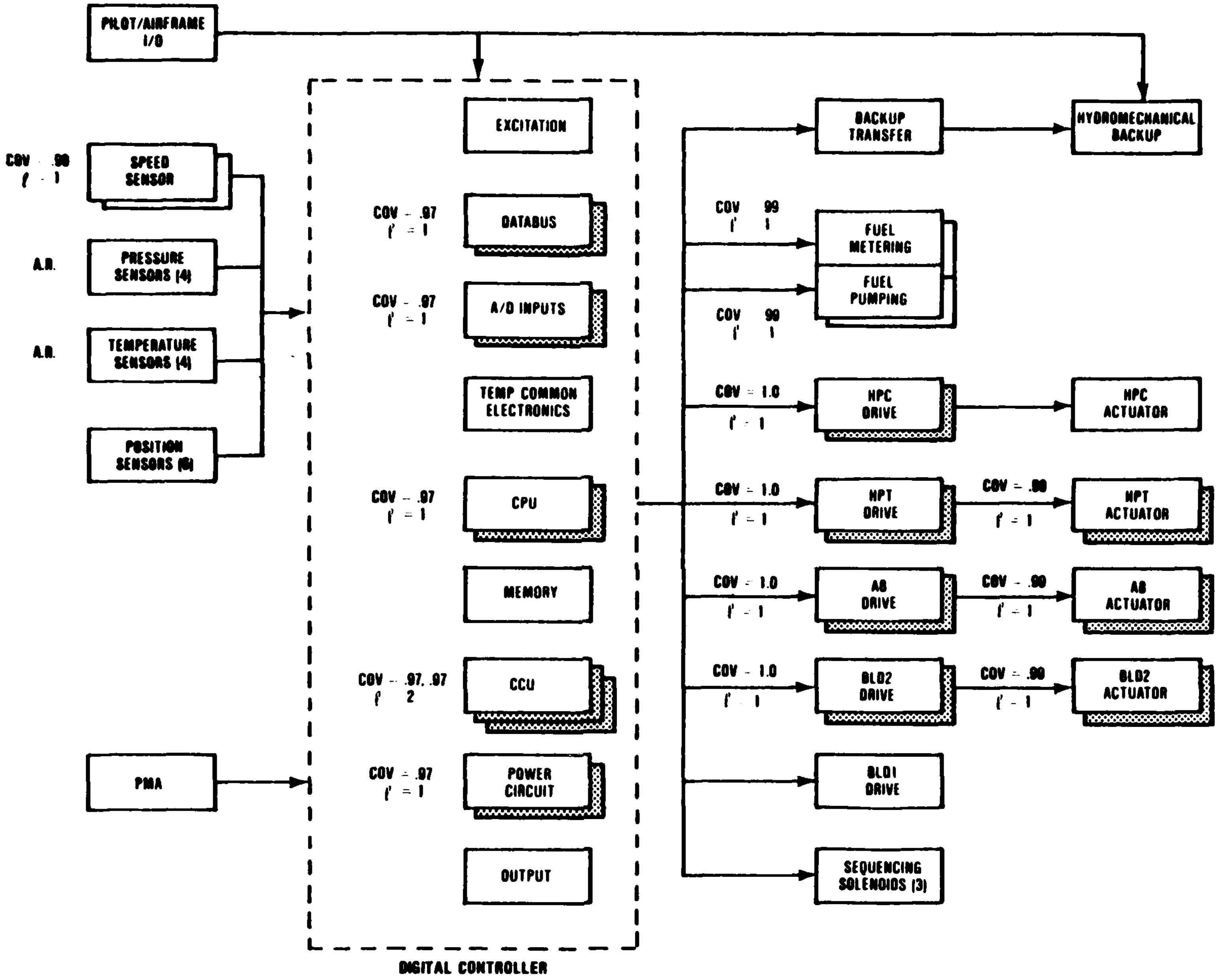


Figure 13. FAFTEEC Derivative Control System

sents a triplex module. An example of this is the CCU module in the digital controller. The notation A.R. indicates analytical redundancy used for the pressure and temperature sensors.

For each module utilizing redundancy, coverage values are assigned. Single coverage values exist for duplex modules while a pair of coverage values is used for triplex modules. For the pair of coverage values, the first number represents the coverage when no modules are failed while the second value represents the coverage after one module has failed. It should be noted that for some configurations a coverage value of .999 will go to .99 when a triplex module goes to duplex following a failure of the primary active module. This is an indication that the fault recovery method is dependent on redundancy level, such as a voting technique, and that the method's effectiveness reduces directly proportional to the level of replication.

Maintenance levels, when associated with the modules, are an indication of when maintenance is required. A level of 1 indicates maintenance should be done when only one module from an originally redundant configuration is active. A level of 2, as shown with the CCU, indicates that repair should be done when 2 modules of a triplex configuration are healthy. One other module maintenance level, -1, indicates that the module will not be repaired until a system failure associated with the failure of that module has occured.

The only remaining information necessary to completely define a system configuration is any specific subsystem grouping and subsystem or system maintenance policy exercised.

Many such system configurations were evaluated with respect to the system effectiveness goals. Simulations and other analytical tools were used to accomplish these evaluations. Those tools are described in the following section.

SECTION V
FAFTEEC DESIGN TOOLS

The methodology for designing a fault-tolerant system incorporates the utilization of specific design tools. Those used in the FAFTEEC program included a Generalized Reliability and Maintainability Program (GRAMP), a Generalized Reliability and Maintainability Simulator (GRAMS) and a Life Cycle Cost (LCC) analysis procedure. Details of these tools, along with the component data used by these tools, are given in this section. As will be explained, GRAMP was used to screen candidate fault-tolerant system configurations by performing a constant failure rate (CFR) analysis at low cost in order to identify reliability drivers and meet reliability goals through multiple runs. Once desirable configurations had been identified, GRAMS performed a time-varying analysis of each configuration. Inclusion of detailed Air Force deferred, scheduled, and opportunistic maintenance policies in GRAMS provided a more accurate evaluation of the candidate configurations with respect to reliability figures of merit (MTBF, MTBR, MTBUR) and with respect to operating costs due to maintenance events. Finally the LCC procedure detailed the operating expenses for selected fault-tolerant system designs over a 15 year operation period for a given fleet size. Realistic field data was accumulated for all control components. This data was used in GRAMP, GRAMS, and LCC to determine the success of candidate fault-tolerant designs in satisfying system effectiveness goals .

1. GENERALIZED RELIABILITY AND MAINTAINABILITY PROGRAM (GRAMP)

Historically, mathematical models have been an essential tool in the evaluation of fault tolerant designs. These techniques compute system reliabilities based on configuration, hardware failure rates, mission time, and coverage. Markov models are particularly applicable because they facilitate reliability estimation for a wide range of systems that are characterized by permanent as well as transient fault recovery capabilities. Incorporation of additional states associated with repair allows the extension of the analysis to repairable systems.

Fault tolerant systems are typically defined in terms of subsystems (e.g. memories, processors, I/O boards, etc.). Each subsystem may consist of a set of identical modules classified as active or spare (in the FAFTEEC application all spare modules will be designed as powered). In a closed system (i.e. without manual repair), each module can be in three possible states:

- Active operating state (i.e. currently participating)
- Spare state (i.e. powered and available)
- Failed state

Under a closed system, fault tolerance can be achieved through some level of system redundancy. Upon module failure, the system must reconfigure to recover from the failure. The capability of this recovery mechanism is measured by the system's coverage. In analysis with the Markov model the system is specified via a finite number of states. Each represents a subsystem configuration that is either operational ("good") or failed. The usual strategy is to represent all possible failed states by a single absorbing state. A transition out of a good state occurs when a module fails. If recovery from this failure is successful, transition is made to another good state. Unsuccessful recovery results in transition to the failed state. Graceful degradation can be modeled by identifying states where the system is operational with a moderate loss of system capability (e.g. reduction in the set of active modules). Full operation is dependent on the survival/recovery of all subsystems (i.e. subsystems in series). This implies that system reliability is a product of the subsystem reliabilities. By decomposing the system into these subsystems and posing the subsystem as Markov models, their reliability can be evaluated. This allows the identification of subsystems most affecting the overall system reliability.

(a) GRAMP Structure

The structure of GRAMP consists of three parts: two Markov models called the Cost Evaluator Model (CEM) and the Reliability/Feasibility Model (RFM), and a third structure linking the two Markov models. The CEM and RFM are run on specified independent subsystems of the system to be modeled so as to reduce the number of components being modeled simultaneously. Since the number of states in the Markov model increases exponentially with the number of components, the fewer the number of modules in a subsystem, the better.

The following describes the two-Markov model structures in GRAMP. Given a subsystem design, input parameters, and a stationary (independent of time) maintenance policy, the cost evaluator model is invoked to solve for the steady state probabilities of being in various states. Average cost per unit time is also evaluated, thus the title CEM.

The CEM models a repairable system which is being evaluated over an infinite time horizon. The expected system performance is found, assuming it has been operating long enough to reach steady state, under a maintenance policy which depends only on the state of the system, not on time. These steady state probabilities are then used to compute CEM output as well as the initial operating conditions for the reliability/feasibility model (RFM).

The CEM is an approximation of reality in order to take advantage of the simple solution for a continuous time Markov process. In reality, opportunities for repairing the fault-tolerant system occur after every mission, that is at discrete time intervals. In the CEM, the repair opportunity occurs at the instant of the state transition or component failure rather than at the end of a mission. Due to the shortness of missions (3 hrs) compared to the mean times between failure of FAFTEEC modules (4,000 to 400,000 hrs), the likelihood of more than one failure per mission is extremely small; hence the continuous time approximation is valid.

The need for the second Markov model, the RFM, is precipitated by the requirement for evaluation of reliability over time. The RFM is a dynamic model of a closed (nonrepairable) system. It assumes the initial conditions on the system components are the steady state probabilities generated from the CEM.

Then the RFM computes reliabilities for fixed-time missions, assuming no repair is done during the mission. This system reliability is then compared to a standard to determine whether or not a given system design along with specified maintenance is a "feasible" configuration in terms of a reliability goal. Table 4 summarizes charcteristics of the CEM and RFM. Both the CEM and RFM can be run independently.

Table 4. Summary of CEM/RFM Characteristics in GRAMP

	Cost Evaluator Model	Reliability/Feasibility Model
Model Type	Markov	Markov
Repair	Yes	No
Solution	Static	Dynamic
Initial Conditions	Irrelevant - steady state solution	From input and/or CEM
Output	Cost steady state behavior	Reliability over specified mission lengtn

The third part of GRAMP is the structure connecting the CEM and RFM which consists mainly of system bookkeeping of subsystem results from each model plus the use of the CEM steady state probabilities in computing RFM initial conditions. System bookkeeping involves simple mathematical combinations of detailed subsystem outputs produced by the Markov models to produce system results. For such bookkeeping to be possible, the subsystems must be chosen to be independent and in series, that is the system fails whenever one of the subsystems fails. To determine system reliability the subsystem results are multiplied, and to determine system costs the subsystem results are added.

(b) GRAMP Assumptions

Table 5 summarizes the basic underlying assumptions required to use the GRAMP model.

The three key system assumptions required for model formulation as a Markov process are that the components are independent (failure of one does not induce failures in others), that they are stochastically deteriorating and that they have constant or piecewise constant failure rates. Other system assumptions are that the components are either working or failed (no graceful degradation) and that a state transition in the Markov model immediately follows a component failure. Transition points for states could have been defined in several ways, however when defined as above, the most mathematically tractable results can be obtained using CSRM theory.

The second key assumption is maintenance related. Restrictions to stationary maintenance policies (ones which do not depend on time, only on the configurations of the components and the assumption that repair brings a component back to its original condition) are not crucial in formulating a Markov model for the system. However, they are necessary in keeping the possible number of states to a size permitting solution. The assumptions of instantaneous repair, failure detection and recovery times and unlimited service capacity could be easily relaxed with moderate modification to the current GRAMP code. However, for FAFTEEC purposes, these assumptions approximate reality while simplifying the analysis.

The restriction of maintenance actions to the times of component failures, thus allowing for a continuous time formulation and solution of the problem, has been previously discussed. Otherwise the problem would be in discrete time requiring a much greater computational effort to solve. Possibilities of multiple failures within 3 hour missions would lead to increased density of cause transition matrices.

Table 5. GRAMP Underlying Assumptions

The System

- Stochastically deteriorating*
- Independent components*
- (Piecewise) Constant failure rates*
- State transition immediately following component failure
- Components either working or failed

Maintenance

- Stationary maintenance policies+
- Repair brings component back to "new" condition+
- Maintenance actions at instant of component failure
- Instantaneous repair, unlimited capacity
- Instantaneous detection and recovery from failures

Time Clock

- Continuous time
- CEM, time invariant
- RFM, time variant

* = crucial assumption for Markov models

+ = necessary for workable number of states in model

The third assumption deals specifically with time clock. The time clock on the CEM and RFM models is continuous. For the CEM, the planning horizon is infinite for computing steady state average results. In contrast, the RFM solves for results over a discrete fixed mission length given an initial condition either user-specified or provided by the CEM.

(c) GRAMP Input

In order to perform a reliability analysis the system must be functionally divided into subsystems and modules. Modules are a replicable set of elements performing a specified function chosen to be modeled as a unit. Failures in different modules must be statistically independent.

Modules are chosen to be building blocks for the system upon which system design, input data and maintenance policies are based. These must be selected carefully based on engineering judgement and knowledge of the system to be modeled.

On the other hand, subsystems are simply sets of modules chosen to be grouped together. Subsystems must be independent and in series. If all modules are independent and in series, then each subsystem consists of a single module. Possible reasons for including modules in the same subsystems include analytical redundancy among certain modules and simultaneous maintenance desired on a group of modules.

Input to GRAMP is on a system, subsystem, and module basis. System input includes costs for system failure (penalty charge) and fixed charge for repair, as well as a number of variables providing options on running various features of GRAMP such as the CEM, RFM, or plots. Various print levels and options for output are also specified in system input.

Subsystem input specifies which modules are to be modeled together as well as which modules must be operational for continued subsystem performance. These sets of modules are called critical sets. These critical sets need not be disjoint.

Table 6 illustrates the specific input required in the FAFTEEC analysis.

Table 6. GRAMP Input Summary

System

I. Fixed charge for repair
II. Failure charge for breakdown
III. Run options
IV. Print options
V. Mission length

Subsystem

I. Number of modules in subsystem
II. Reliability requirement
III. Repair decision during preventative maintenance
IV. Analytical Redundancy (pressures, temperatures)

Module Definition Parameters

I. Maintenance level
II. Redundancy level
III. Replacement level
IV. Sensitivities to compute
V. Failure rates
VI. Coverage
Active
Spare
VII. Coverage strategy

(d) GRAMP Output

Given the probabilistic structure and assumptions of the GRAMP Markov model, much useful information can be generated to evaluate trade-offs between varying system objectives. Included in the ouptut are mean times between or to various events as well as the number of events per million hours. Events considered are:

(1) Any maintenance
(2) Preventative maintenance
(3) Unscheduled repairs
(4) Any failure
(5) Failure due to coverage

All of these events occur on either a module or a subsystem basis.

Output is generated from both the RFM and the CEM. The latter is discussed first. After solving for the steady state transition probabilities the CEM calculates for all the events the number per million hours and the mean times between occurrences.

The O&S cost per hour for the subsystem is divided into its contributing factors: system penalty cost, fixed charge for repair and replacement charge on a module basis. Sensitivities of all of the above quantities with respect to module failure rates, repair charges, and coverages can be computed, if so specified by the user. Weight and acquisition costs are computed through simple addition of module, component, and system cost values.

RFM output is limited only to reliabilities and mean times until failure events because of the no maintenance assumption. Output from the RFM due to its dynamic nature varies with time. Time steps for which results are computed are part of the user input as are flags to generate reliability or MTTF history time plots. CEM and RFM results are determined only for subsystems. A separate section computes system values for key objectives and prints a summary of system and subsystem results. Table 7 summarizes the output that is available from GRAMP.

Table 7. GRAMP Output Summary

CEM (on a module or subsystem basis)

- Failure/maintenance events per million hours
- Mean time between events
- Relative O&S costs
- Acquisition costs
- Weight
- Sensitivities

RFM (module or subsystem basis)

- Reliability
- Mean times to failure
- Reliability time history plot

System Summary (system basis)

- Reliability
- MTTF
- O&S and acquisition costs
- Weight
- CEM events per million hours (abort rate)
- MTBF, MTBR
- Subsystem summaries

2. GENERALIZED RELIABILITY AND MAINTAINABILITY SIMULATION (GRAMS)

Monte Carlo simulations are routinely used for reliability analysis of complex systems. These systems are characterized by conditional failure events, redundant configurations, components with time-varying failure rates, as well as complicated maintenance/logistics procedures. The underlying procedure is to formulate a stochastic process that is essentially identical to the system under study. The key assumption of the model is that the distribution functions of various events (e.g. successful operation, failure, maintenance) are known or can be approximated. Choosing a random number uniformly distributed between 0 and 1, generates a value from the cumulative distribution that corresponds to the outcome of a Monte Carlo experiment (e.g. time to first failure, time to repair).

For the FAFTEEC application a fault tree was used to formulate the underlying structure of the simulation. This ensured that the event sequence was preserved. Fault-tolerant system behavior was simulated by tracing the operation through the fault tree in accordance with the probabilities associated with each event. The results from each trial (e.g. event history, operating time, failure modes, cost incurred, etc.) were recorded and regarded as "experimental data". The simulation was repeated until the experimental data sufficiently represents a statistically constant result.

The Generalized Reliability and Maintainability Simulation (GRAMS) was used to accomplish the time-varying analysis. This analysis simulates individual engines (hosts) and their controllers (systems) through a fifteen year life cycle using Monte Carlo methods. GRAMS includes nonconstant failure rates and a more detailed maintenance philosophy than GRAMP.

(a) GRAMS Structure

As previously stated GRAMS is a Monte Carlo discrete event digital simulation which models system failure and repair during a 15 year life cycle. It is a combination "time slice" and "next event" simulation. The latter method computes times of failure and repair events prior to the start of the simulation. The simulation then proceeds from one event to the next based upon these computed times. The "time slice" method determines whether or not an event occurs at each time step utilizing a binominal experiment. The program is designed to simulate failures in a large number of systems and compute expected values for time between failures, time between repairs and Operating and Support (O&S) costs. Incorporated in the simulation is the capability to handle failures due to two discrete events such as lightning and maximum temperature as well as normal module failures during a mix of missions of two lengths (3 hours and 10 hours). The dynamic maintenance policies include unscheduled, scheduled, opportunistic and deferred maintenance for both shop and line repair.

Within GRAMS, failures can occur due to natural module failures based on their piecewise constant failure rates, module switching failures based on their coverage values or module failures based on the occurrence of discrete events such as lightning or maximum temperature. Independent component failures are determined by random events.

The maintenance strategy is inexorably tied to engine mission, operations, and support. The digital electronic controls are intended to operate in a single/dual engine tactical fighter environment. Actuarial data collected by the Air Force reveals that these engines routinely experience removals on the order of 150 hours. Whenever an engine is removed for a non-control related fault, an opportunity exists to perform a preventative maintenance action on the controls. It also impacts the decision to defer noncritical system maintenance as well. This relationship between the engine (host) and the fault-tolerant control system is an important element of the time varying simulation.

(b) GRAMS Assumptions

Certain assumptions are made in GRAMS relative to methods for computing mean time between failure (MTBF) in hours, mean time between repair (MTBR) in hours, reliability (REL) and system failure rate (ABORT) in failures per million hours (FPMH). These methods are documented below.

$$\text{MTBF} = \frac{\text{\# engines x hours per interval}}{\text{\# failures per interval}}$$

$$\text{MTBR}_i = \frac{\text{\# engines x hours per interval}}{\text{\# repairs of type}_i}$$

$$\text{REL}_j = \frac{\text{\# failures during mission type}_j}{\text{\# missions of type}_j}$$

$$\text{ABORT} = \frac{\text{\# failures x } 10^6}{\text{\# engines x hours per interval}}$$

With respect to maintenance the model has been developed to allow flexible definition of maintenance strategies that may be design specific. These include the capability to set usage limits for components and preventative maintenance repair levels for redundant modules.

There are four repair level policies that are specified for GRAMS. Levels 1 and 2 are subsystem related while levels 3 and 4 are module related.

Level 1 is to repair only failed module components that caused subsystem failure.

Level 2 is to repair all the failed components in that subsystem.

Level 3 is to repair all module components which are within a specified screening interval of their maximum operating times. Different intervals can be applied to installed or uninstalled units.

Level 4 is to repair all failed components in a module if the number of redundant components minus the number of failed components is less than or equal to a specified module value.

GRAMS models an engine independent of the controller. This allows accurate interpretation of maintenance philosophies as they affect MTBR. At the successful end of a mission or following a mission abort, maintenance can be performed on the system. Events include:

- o component failure
- o engine failure
- o component MOT's
- o discrete events (Lightning/EMI/RFI/Max. temperature)

Whenever an engine requires removal, both the engine and fault-tolerant control system are sent as one entity to the base shop, where opportunistic maintenance can occur. At the shop, level 1 and level 2 repair policies are applied as specified for each subsystem. Once these repairs are complete, level 3 repairs are done using a screening interval to determine component replacements. Next, level 4 policy is applied to modules with specified deferred maintenance.

If the engine does not require removal and no events have occurred inflight, a level 4 inspection follows each mission. Line replaceable units (LRU) are repaired on the wing.

The fault-tolerant system is sent to the shop if it fails the inspection for any non-LRU module. Repair is done as described above. False alarms requiring unnecessary removals are also generated.

If the engine does not require removal and an event has occurred, level 3 repairs are checked. If they are not LRU, the fault-tolerant system is also sent to the shop. If no shop repair is required and the system has not failed, level 4 (end of flight) inspections are done as described above. If the system has failed due to any of the discrete events, the fault-tolerant system is automatically returned to the shop. Otherwise, the system failure must be attributred to a component failure. Levels 1 and 2 are done only for the failed subsystem. If they are LRU, repair is performed at the flight line. If they are not LRU, the fault-tolerant system is returned to the shop.

Because modules considered in the FAFTEEC analysis had failure rates in the range of 10^{-4} and 10^{-6} per hour (10,000 to 1,000,000 experiments run for one failure), special techniques were incorporated in GRAMS for variance reduction through sampling and confidence interval determination.

For GRAMS a technique was chosen that would predetermine when component failures were most likely to happen. Binominal experiments were run at these points, and the FAFTEEC status changed as required. Although not explicitly a variance reduction technique this procedure greatly improved the efficiency of the simulation. A sufficient number of runs could then be made within a reasonable CPU time so that the results were statistically acceptable.

(c) GRAMS Input

As with GRAMP input to GRAMS is done on a system, subsystem and module basis.

At the system level, cost data, event probablity data and maximum operating time data must be provided. The following seven penalty costs are associated with various maintenance actions:

(1) The cost of required maintenance on the back-up controller when it fails its pre-flight inspection.

(2) The cost incurred when the switching mechanism for the back-up controller fails after the digital controller has failed.

(3) The cost of opportunistic maintenance done on one or more components which were repaired while the engine was in shop for reaching its MOT or for scheduled maintenance.

(4) The cost incurred whenever scheduled flight line maintenance is done.

(5) The cost incurred whenever unscheduled flight line maintenance is done.

The above items should include man-hour costs to inspect remove, clean, repair, and test the controller; maintenance equipment costs; facility costs; and other associated overhead costs.

The following event probabilities are needed on the system level:

(1) The probability of a particular mission type (3 hour/10 hour).

(2) The probability of doing end of flight maintenance even when not required due to improper diagnostic operation.

(3) The probability of not doing end of flight maintenance even when required due to improper diagnostic operation.

(4) The probability of both maximum temperature and lightning events.

(5) The probability of each level of severity (n of them) for both maximum temperature and lightning events.

(6) The probability of engine failure on a mission.

(7) The probability of backup inspection failures.

(8) The probability of backup switching failures

In addition, the number of engine operating hours (lifetime and per year), the lengths of mission A and B in hours and the number of severity levels for lighning and maximum temperature events, the number of engines to be simulated, the number of engines in the fleet, and the array of times for failure rate data must be provided. The confidence interval calculations require input for the engine population and the minimum and maximum number of engines. Output pages are determined by specifying a print level or specific list options.

Maximum operating time data on the system consists of the engine MOT and the component MOT screening intervals for both installed systems and systems in for shop repair.

At the subsystem level, data must be provided as to which of the 41 modules constitute each subsystem and whether or not that subsystem consists of line replaceable units. In addition, critical sets of modules for each subsystem are defined as well as subsystem maintenance strategies.

At the module level, cost data, event probability data, MOT data, time varying failure rate data, and redundancy data must be supplied. Maintenance strategies for each module are also needed. For each module whenever a component is repaired/replaced, a cost is incurred which includes the actual cost of the component (the cost to purchase/acquire it) plus the cost of the man-hours to remove the failed component and replace it with a working unit. For each module, the probability of failure for each of the severity levels for both maximum temperature and lightning events is desirable. In addition, the maximum operating times (e.g. "throw-away" modules) and time varying failure rates for each of the modules must be provided in order to complete the final configuration evaluations with GRAMS.

(d) GRAMS Output

This section documents the output list options (LO) of GRAMS. There are 19 possible list options of output and 7 print levels (LEVP). In addition to the print levels, the user may specify each list option of output that he would like printed (LOPS). Table 8 identifies the list options for each print level.

LOs 1 through 4 list the simulation definition parameters for input verification. LO 5 gives the yearly and aggregate per-engine system results: reli-

Table 8. GRAMS Output Summary

		Print Options						
Page	Title	1	2	3	4	5	6	7
1	Namelist Input	X	X	X	X	X	X	X
2	Parameter Definitions	X	X	X	X	X	X	X
3	Subsystem Definitions		X	X	X	X	X	X
4	Module Definitions				X	X	X	X
5	System Results	X	X	X	X	X	X	X
6	Subsystem Reliability		X	X	X	X	X	X
7	Subsystem MTBF		X	X	X	X	X	X
8	Module MTBF Due to Component Failure Module MTBF Due to Coverage Failure				X	X	X	X
9	System MTBR by Maintenance Type	X	X	X	X	X	X	X
10	MTBR Driven by Subsystem Maintenance (Average over engine life)		X	X	X	X	X	X
11	MTBR Driven by Subsystem Maintenance (Yearly Average)			X	X	X	X	X
12	Events Driven by Subsystem Maintenance (Yearly average over engine life)				X	X	X	X
13	Events Driven by Subsystem Maintenance (Yearly)					X	X	X
14	O&S Cost Breakdown (Percent over Life Cycle)	X	X	X	X	X	X	X
15	Component Replacements by Maintenance Type (Yearly average over Life Cycle)						X	X
16	Component Replacements by Maintenance Type (Yearly)							X
17	Component Replacements Attributed to Maintenance Plan (Yearly & Aggregate)						X	X
18	Backup Failures		X	X	X	X	X	X
19	Print Option Definitions		X	X	X	X	X	X

ability for both mission types, abort rate (FPMH), mean time between failures (MTBF), and operation & support (O&S) costs per hour ($). LO 6 and LO 7 provide the yearly per-engine subsystem reliability and MTBF. LO 8 lists both the module MTBF due to coverage and due to component failures on a per-engine basis.

LOs 9 through 17 deal with maintenance actions. LO 9 lists the system mean time between repair (MTBR) by maintenance type per engine. These repair types are either opportunistic because of supersystem (e.g. engine) repair, schedule LRU, scheduled shop, unscheduled LRU or unscheduled shop.

LO 10 gives the average MTBR per engine over the life cycle driven by subsystem maintenance. Subsystem maintenance actions occur in shop or at the flight line because either a subsystem fails, a maximum operating time is reached, or a preventative maintenance limit is reached. LO 11 output is similar to LO 10, except it gives the results year by year.

LO 12 and LO 13 list the number of events on a fleetwide basis driven by subsystem maintenance on a modular basis. These maintenance events are scheduled or unscheduled, shop or flight line, and are driven by subsystem failures or preventative maintenance action. LO 12 and LO 13 are yearly averages over the engine life and yearly figures, respectively.

LO 14 is the operation and support cost breakdown per engine as a percentage over the life cycle. Unscheduled, scheduled and additional opportunities (those not due to supersystem/engine maintenance) are broken down into shop visit and LRU replacement costs. These costs are further divided into the basic charge for the visit or repair and the component removal and replacement costs. The engine opportunistic column refers to opportunities to do FAFTEEC maintenance while the supersystem (engine) itself is being repaired. These repairs are done only at the shop. The additional opportunistic column refers to additional FAFTEEC maintenance opportunities due to FAFTEEC primary driver repairs. There are no basic charges associated with additional opportunistic maintenance.

LO 15 and LO 16 list the number of component replacements on a fleetwide basis by maintenance type on a yearly life cycle average basis and a yearly count basis, respectively; again, the maintenance types are scheduled, unscheduled, engine opportunistic and additional opportunistic. They are further divided by module type, that is whether the module is defined to be an LRU or shop replaceable unit.

LO 17 gives the number of components of each module type for all engines simulated that are replaced under each of the four maintenance plans for each year and as an aggregate total.

LO 18 refers to backup control failures and gives the total number of yearly and aggregate failures detected by either switching or inspections on a fleetwide basis.

LO 19 documents the output pages printed under each of the available print options.

3. LIFE CYCLE COST (LCC) PROCEDURE

A Cost of Ownership analysis was identified as a major FAFTEEC item to address sensitivity of Life Cycle Cost (LCC) to various parameters such as maintenance plans and reliability projections. The overall analysis relied on the conceptual techniques used successfully in the Turbine Engine Technology Demonstrator Component Development program (USAF Contract F33657-73-C-0618) and Reduced Cost Turbine Engine Concept (RCTEC) program (USAF Contract F33675-77-C-0425). The use of this technique was necessary to allow initial sensitivity studies to be done for various control maintenance plans, failure modes, and operational rules (e.g., a mission may be initiated when one sensor in a redundant set is known to be inoperative since the probabilty of another failure within the mission time causing an in-flight shutdown or mission abort is remote.)

Trade studies assessed the probable improvement in reliability versus the change in acquisition cost and maintenance cost for contemplated fault-tolerant control system configurations. DDA established a cost of ownership model for a baseline system. A statistical anaysis projected appropriate characteristic life and failure mode for each evaluation. These data, coupled with impact on various levels of maintenance, and acquisition costs were combined to calculate a relative Cost-of-Ownership figure of merit.

Program input data relied on USAF planning documents and on performance, reliability, and maintainability information. Typical of these factors are military labor rates, maintenance turnaround times, and maintenance level destination percentages for unscheduled maintenance actions.

(a) LCC Approach

The term Life Cycle Cost (LCC) is generally defined to mean the summation of all RDT&E, acquisition, operating, and disposal costs. In practice, many elements from these categories are very small contributors to LCC although critically important to the success of the program. Other elements may be essentially the same magnitude regardless of certain program variables such as a tire size or even the nature of the aircraft engine control. This practical approach was supported during a combined USAF/Industry working group effort during the RCTEC program. Members of the USAF/Industry working group were charged with developing an aircraft engine LCC model which addressed all elements of engine LCC. This task was accomplished in 1975/1976 and reported 1 February 1977. One aspect of the work in 1976 resulted in each of the team groups estimating the relative percentage contribution of each LCC equation. The results of these estimates are shown in Table 9

Table 9. LCC Relative Cost Contribution Summary

Category	Program Phase and Percent of Phase LCC		
	RDT&E	Acquisition	Operating & Support
Detail Design Cost	15		
Tooling Cost	5	5	
Fabrication			
Engines	36	64	
Spares		25	
Contractor Test	28		
System Engineering	7		
Packaging & Shipping			7
Scheduled Maintenance			
Unscheduled Maintenance			62
Petroleum, Oil, Lubricants			27
	91%	94%	96%

The percentage of LCC captured is generally recognized to be sensitive enough for early trade studies. Programs involving fighter or attack aircraft programs usually find acquisition cost several times RDT&E. Operation and support costs generally approach but do not exceed acquisition cost. This weighting would indicate that about 93 - 94% of LCC is captured by the equation categories listed in Table 9. Bomber or transport aircraft programs also usually find acquisition cost several times more than RDT&E. However, operation and support costs often exceed acquisition by two or three times. Therefore about 95% of LCC appears to be captured.

Several important program elements were omitted from the system LCC equation set since they were considered relatively low cost drivers. These elements were: mockup, peculiar support equipment, common support equipment, special test equipment, facilities, government testing, training, contractor field support, data, initial inventory management, recurring inventory management, recurring maintenance management data, and production program start-up. One example to support the rationale for exempting these program elements might be appropriate. Training, for example, is necessary for any equipment. However the absolute cost of specific course material is relatively low when compared to the entire program and the number of people to be trained over the life of a program is principally a function of personnel turnover. Therefore, the absolute LCC difference driver is essentially the length of the course and cost of consummable trainer aids.

Acquisition and RDT&E elements were recognized. Not only were differences in production cost recognized, but the anticipated development difficulty was sized in terms of cost. These values yielded variances in acquisition and RDT&E which, when combined with operating and support cost factors, summed to the LCC figure of merit.

(b) Use of Life Cycle Costs

LCC was used as a figure of merit for each of the fault-tolerant control configurations and maintenance philosophies developed during FAFTEEC. LCC factors were estimated for various maintenance levels based on knowledge of the USAF logistic support system (Figure 14).

Potential maintenance plans were drawn such as the one shown in Table 10. In addition to scheduled and unscheduled maintenance, analytical provision for opportunistic and/or deferred maintenance was added to the LCC analysis.

These factors were combined with cost values representing labor, investment spares, and material usage rates at all probable maintenance levels (Table 11). Frequency of occurrence (a measure of durability) was simulated to allow calculation of LCC sensitive to the maintenance plan and design characteristics of the control system in a reference airframe.

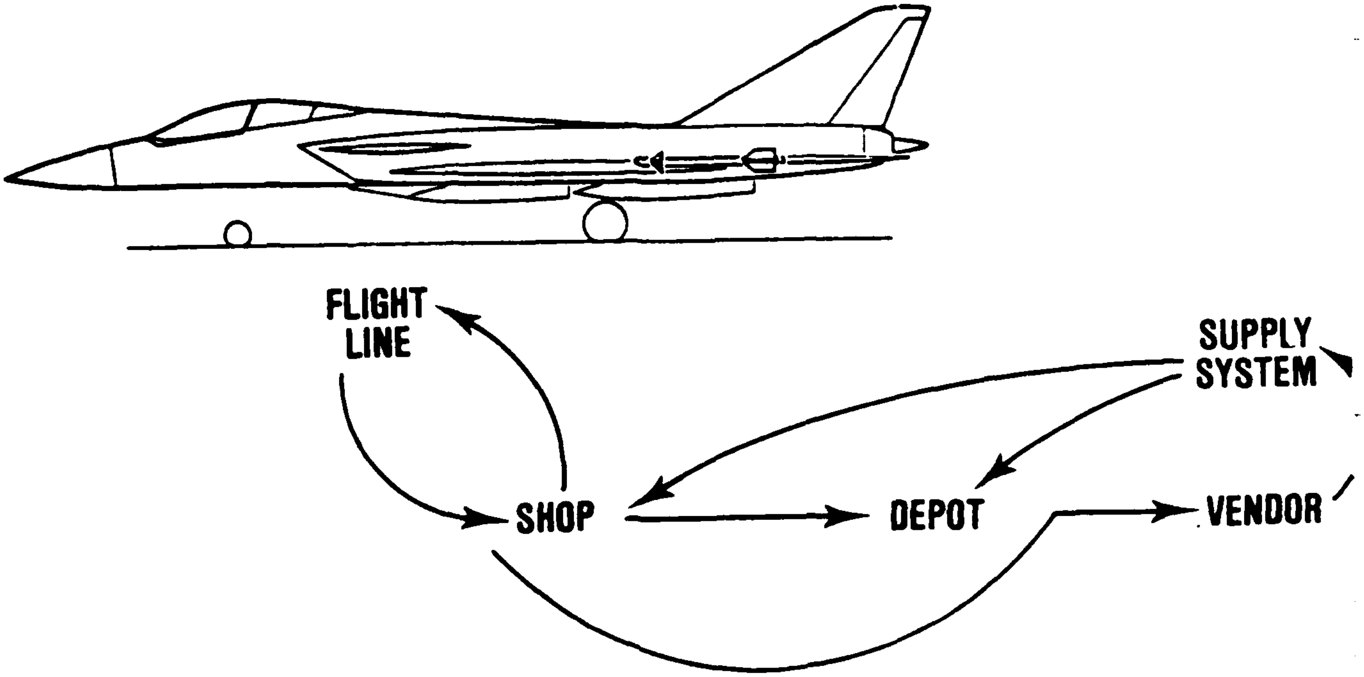


Figure 14. General Maintenance Flow

Table 10. Potential Maintenance Responsibility Levels in FAFTEEC

	FLIGHT LINE	BASE	DEPOT	VENDOR
SCHEDULED	✓	✓	✓	
UNSCHEDULED	✓	✓	✓	✓
OPPORTUNISTIC		✓	✓	
DEFERRED		✓		

Table 11. LCC Operating and Support Considerations

OPERATING & SUPPORT CONSIDERATIONS	
MAINTENANCE LEVELS • PLAN • DEPOT •OVERHAUL • MAJOR REPAIR • BASE SHOP • MAJOR REPAIR • MINOR REPAIR • FLIGHT LINE • LINE REPLACEABLE UNIT • ADJUST • COST FACTORS AT EACH LEVEL • LABOR • MATERIAL • USAGE RATES	DURABILITY • SCHEDULED MAINTENANCE • UNSCHEDULED MAINTENANCE • PREMATURE REMOVAL • OPPORTUNISTIC • REDUNDANT FEATURES • COVERAGE

Fault-tolerant system configurations were compared to a known hydro-mechanical control reference. FAFTEEC factors were used to calculate an advanced technology reference control. Then variables, (e.g. redundancy, coverage, quality of parts, maintenance variances) could be evaluated relative to the baseline figure of merit. A variant figure of merit was then determined for each configuration of interest in terms of relative LCC.

(c) Life Cycle Cost Computation

During the FAFTEEC configuration analysis Life Cycle Costs were computed for promising candidate designs. This computation procedure used concepts from the two previously developed cost models (described in Appendix 4) complied with failure event histories from the GRAMS model. Figure 15 shows the basic flow of LCC calculations for the three major cost categories.

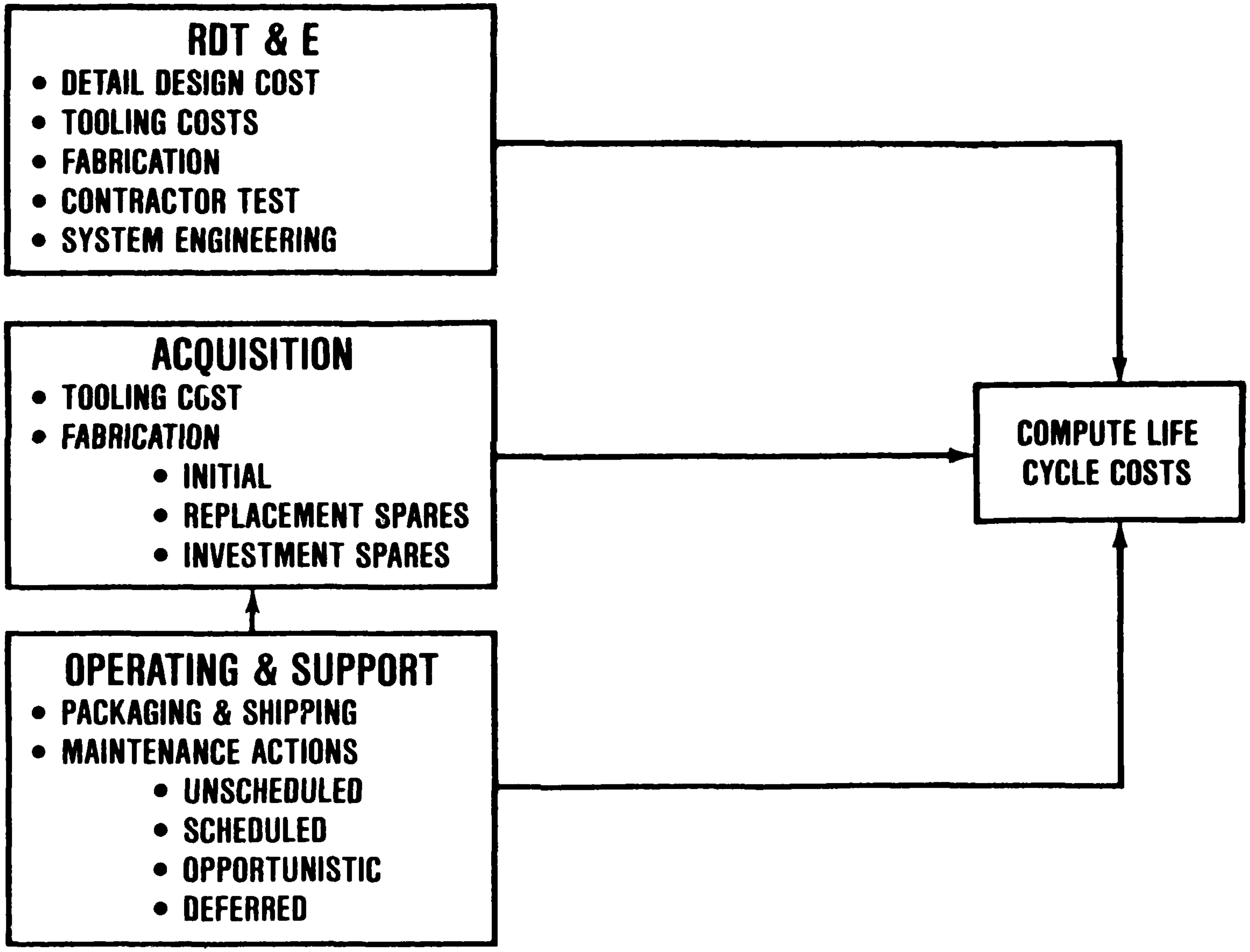


Figure 15. Life Cycle Cost Computation Procedure

4. COMPONENT DATA REQUIREMENTS

An integral and critical element in the FAFTEEC program was realistic and usable reliability data that would permit quantitative assessment of system reliability for various alternate architectures and redundancy approaches. A realistic data base was necessary to assure representative study results, including sensitivities for various system mechanizations under study. Use of MIL handbook piece part failure data was not considered adequate. Deficiencies of these data included inadequate consideration of component stresses on a real design operating environment, and constraint to constant failure rates independent of application. Further, the benefits or disadvantages of various production techniques, e.g., type of stress testing or burn-in, were not recognizable in the handbook data. Therefore, it was decided to utilize an extensive empirical reliability data base collected by Delco Electronics and DDA during many years of actual operating use. Supplemental data was solicited from their vendors. Table 12 shows the primary data sources for the various type of control hardware.

Table 12. FAFTEEC Data Sources

Component	Data Source
Fuel Systems	DDA and Vendors
Actuators	DDA and Vendors
Electromechanical-Servos	Vendors
PMG Excitors, Igniters, Wiring and Connectors	DDA and Vendors
Sensors	DDA and Vendors
Electronic Components	Delco, BNR, and Vendors

The most critical, and substantiated reliability data base was for Aerospace electronic components. This data was largely provided by Delco Electronics. A voluminous data set derived from the extremely high volume, rapidly expanding automotive application provided General Motors, through the Delco Electronics Division, was also utilized.

(a). Data Reduction/Analysis

The approach taken to accumulation of data was to characterize the baseline control system for GMA200 (Section III) in terms of components and modules. Table 1 showed the FAFTEEC Baseline System and its 41 distinct functional modules. The approach to analyzing system designs consisting of these functional modules was to identify like components from items with a substantial data base (GRAMP analysis). Past that the idea was to obtain reliability/cost/maintenance data from these components and use this data in conjunction with the FAFTEEC design goals to analyze various sytem configurations (GRAMS/LCC analysis).

Figure 16 summarizes the module information needed for each analysis tool. Appendix B represents the relevant information for all 41 modules presented in this format.

The data accumulation task was divided into accumulation of data representing the digital controller components (electronic) and the components interfacing with the digital controller (non-electronic) as shown in Figure 17. Accumulation of data for these two classes of components will be discussed in the following two sections.

(b). Electronics Data Base

A large current data base of electronic part reliability data was summarized from Delco's commercial and military inertial navigation programs (Carousel IV), missile guidance systems (Titan II Rivet Hawk), a military tactical aircraft computer (F16) and both entertainment and non-entertainment automobile electronic products.

FAFTEEC MODULE:

MODULE INFORMATION USED BY GRAMP

CONSTANT FAILURE RATE   ABORT RATE   UNIT COST   UNIT WEIGHT

MODULE INFORMATION USED BY GRAMS

NONCONSTANT FAILURE RATE (IF APPROPRIATE)   MAX. OPERATING TIME   UNIT COST   UNIT WEIGHT

		TYPICAL REPAIR		
CATEGORY	AT DEPOT	AT BASE	AT FLIGHTLINE	ON AIRCRAFT
%				
$				
MH				

PROBABILITY OF OVERTEMPERATURE EFFECT
LEVEL 1   LEVEL 2

PROBABILITY OF LIGHTNING EFFECT

MODULE INFORMATION USED BY LCC

RDT & E

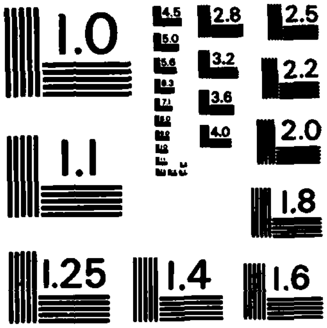
Figure 16. Summary of Necessary Module Information

AD-A121 746   FULL-AUTHORITY FAULT-TOLERANT ELECTRONIC ENGINE CONTROL   2/2
SYSTEM FOR VARIAB..(U) GENERAL MOTORS CORP INDIANAPOLIS
IN DETROIT DIESEL ALLISON DI.. L E BAKER ET AL. APR 82
UNCLASSIFIED   DDA-EDR-10895 AFWAL-TR-82-2037   F/G 21/5   NL

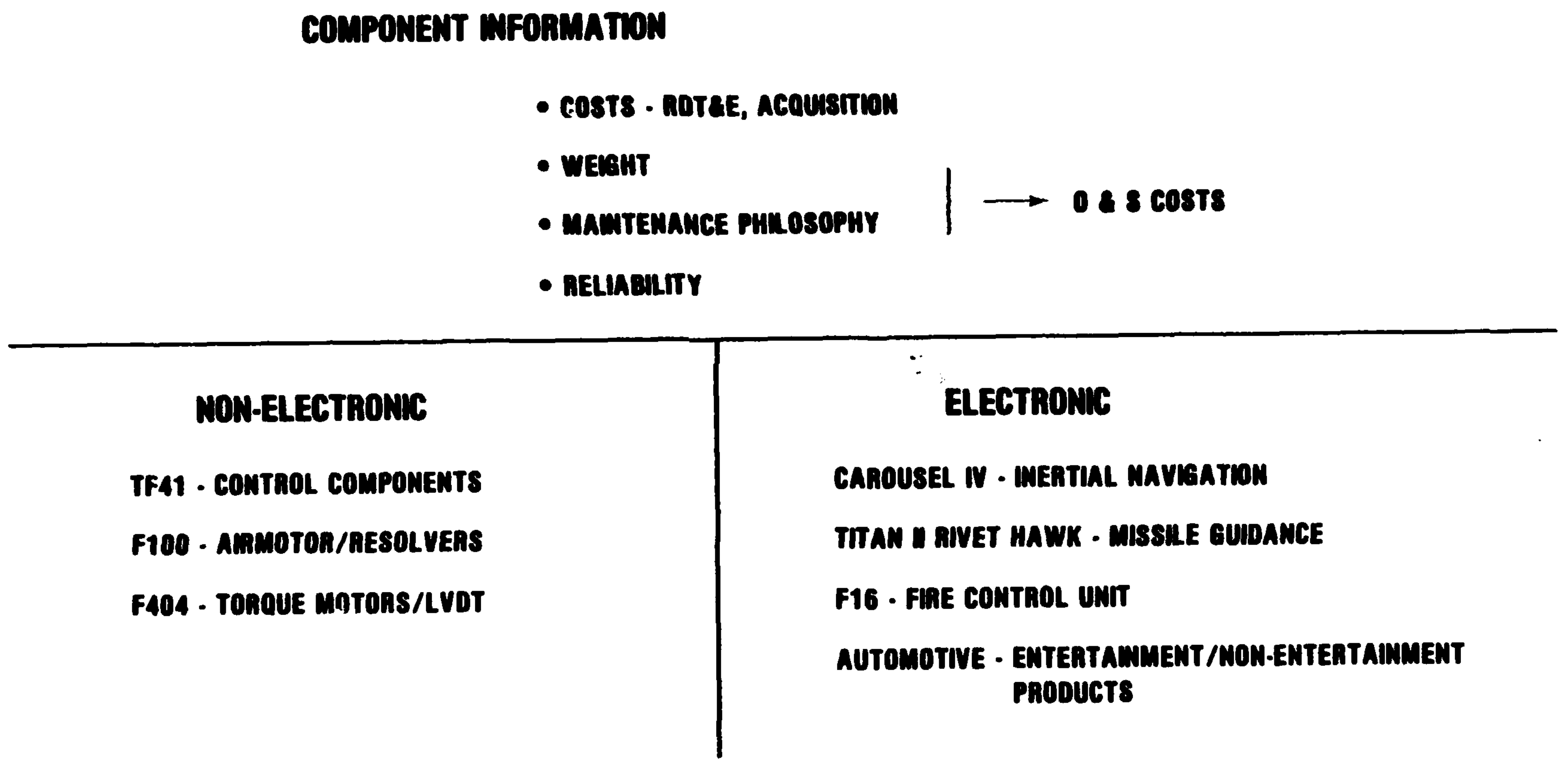
END

FILMED

DTIC



MICROCOPY RESOLUTION TEST CHART
NATIONAL BUREAU OF STANDARDS-1963-A



COMPONENT INFORMATION

- COSTS - RDT&E, ACQUISITION
- WEIGHT
- MAINTENANCE PHILOSOPHY
- RELIABILITY

→ O & S COSTS

NON-ELECTRONIC

TF41 - CONTROL COMPONENTS

F100 - AIRMOTOR/RESOLVERS

F404 - TORQUE MOTORS/LVDT

ELECTRONIC

CAROUSEL IV - INERTIAL NAVIGATION

TITAN II RIVET HAWK - MISSILE GUIDANCE

F16 - FIRE CONTROL UNIT

AUTOMOTIVE - ENTERTAINMENT/NON-ENTERTAINMENT PRODUCTS

Figure 17. Summary of Database Requirements/Sources

The constant failure rate data sources (bulk statistics) covered a wide range of environmental and operating conditions, part technologies, and parts and end item screening practices, none of which completely typified the anticipated FAFTEEC application. A mathematical model was used to relate observed reliability experiences into the anticipated FAFTEEC production and usage scenario. For this purpose, MIL-HDBK-217C, plus more current Rome Air Development Center models, was chosen. Using a graphical format, observed parts failure rates from each data source were compared to that which would be predicted from the math model. These comparisons were reviewed and recommendations were made to either accept the handbook math model or to modify the model with an appropriate multiplying factor.

Delco reliability analysis experience has shown that classical parts count reliability predictions do not adequately account for many of the failure causes of electronic equipments such as assembly workmanship and process deficiencies. Aggregate program statistics reviewed from the several data base sources which show a fairly consistent failure rate ratio between electronic parts and other causes.

The electronic parts reliability data base comparison with MIL-HDBK-217C and RADC-TR-79-97 (RADC) is summarized in Table 13 with recommended experience modifying factors used for FAFTEEC reliability predictions.

MIL-HDBK-217C was found to be grossly pessimistic with respect to virtually all IC failure rate experience and was rejected. The newer IC failure rate models contained in RADC-TR-79-97 were found to fit most experience reasonably well. Discrete semiconductor failure rate experience, on the other hand, was generally higher than predicted by the handbook and appropriate multiplying factors were assigned for the handbook models.

It is noteworthy that commercial plastic encapsulated integrated circuits and other semiconductors perform much better in the automobile environment than would be predicted by the military handbook. These part types were not recommended for FAFTEEC, however, since they are not rated for operation over the full military temperature range.

Table 13. Electronics Failure Rate Experience Factors

PART TYPE	COMMENTS	FAFTEEC RECOMMENDATIONS
INTEGRATED CIRCUITS	o 217C PESSIMISTIC VS. ALL DATA o RADC PROVIDES REASONABLE FIT FOR DIGITAL SSI/MSI o RADC MAY BE SOMEWHAT OPTIMISTIC FOR LINEAR AND LSI DEVICES o RADC PESSIMISTIC FOR COMMERCIAL PLASTIC IC'S	ACCEPT RADC MODELS
DISCRETE SEMICONDUCTORS	o 217C OPTIMISTIC BY 2-5 TIMES FOR MILITARY GRADE PARTS BUT AT LEAST AN ORDER OF MAGNITUDE PESSIMISTIC FOR PLASTICS	MULTIPLY 217C MODELS BY o 3X FOR DIODES AND LOW POWER TRANSISTORS o 5X FOR POWER TRANSISTORS
CAPACITORS		
SOLID TANTALUM	o 217C PROVIDES REASONABLE FIT OF TITAN AND C141 DATA BUT SOMEWHAT OPTIMISTIC RE COMMERCIAL PARTS o CIV DATA MUCH BETTER THAN 217C	ACCEPT 217C MODELS
CERAMIC	o 217C LOW BY FACTOR OF 4 RE CIV AND CIV-E DATA	MULTIPLY 217C BY 4X
RESISTORS	o 217C APPEARS SOMEWHAT OPTIMISTIC FOR CARBON COMP BUT SOMEWHAT PESSIMISTIC FOR THICK FILM NETS o METAL FILM ASSESSMENT NOT COMPLETE	ACCEPT 217C MODELS
TRANSFORMERS/ INDUCTORS	o 217C FITS DATA REASONABLY WELL	ACCEPT 217C MODELS

A major limitation of the available data base was the shortage of experience with large scale integrated circuits such as microprocessors and semiconductor memories. The bulk of the field experience is from earlier generation computers based on small and medium scale IC technologies and magnetic core memories.

Aggregate end item reliability experience from widely dissimilar programs indicated a fairly consistent ratio between the failure rate contribution of electronic parts (2/3) versus all other causes (1/3). Therefore FAFTEEC module failure rates were predicted by multiplying the total parts failure rate by a factor of 1.5 to account for such failure causes as workmanship, process, and design deficiencies.

For each of the FAFTEEC modules associated with the digital controller, data was accumulated at the module level to represent:

- o Module failure rate
- o Module unit weight
- o Module unit cost

The digital controller is not entirely represented (weight-wise, cost-wise, ;ailure rate-wise) by the information for Modules 1-9. The chassis for the controller, while it has no failure rate associated with it, has an appreciable weight (5.5 lb.) contribution. In addition the driver circuits for the torque motors and solenoids reside in the digital control box. Since this is a system study those circuits, and their associated module data inputs, have been included as part of the functional effect in modules with which they interface. This is also true of the encapsulated pressure transducers which reside in the first coded control unit.

Another important consideration is that the failure rates noted here are constant failure rate numbers. This does not necessarily indicate that the constant failure rate assumption is a correct one for electronics - in fact, quite the contrary. Considerable effort was devoted to fitting failure rate information to nonlinear model forms. Both Weibull and Duane models were used in an attempt to fit the data.

Non-constant failure rate characteristics from four divergent electronic equipment applications were studied. In all cases, marked decreases in failure rate were observed versus time. The F16 Fire Control Computer experience was considered most applicable to the FAFTEEC application and was recommended as the empirical model for failure rate versus time modeling. However, the equation for calculating the instantaneous failure rate was considered appropriate for non-redundant modules and most FAFTEEC designs involved replication of modules within the controller, constant failure rate information was used.

(c) Non-Electronics Database

The other 32 modules in the FAFTEEC Baseline System, termed the non-electronic components of the system, were characterized from aircraft engines designated as the TF41, F100, and F404. Data from the latter two applications was obtained from the Energy Controls Division of Bendix Corporation, a valuable contributor to the FAFTEEC program.

The engine control system installed on the TF41 engine produced extensive and well-documented files on all discrete components of the engine control system (including sensors). Failure rates for these components have been derived and their variation with time can be estimated in some instances. The data base, derived from a total experience of over 2.3 Million flight hours, covers a span of ten years. The value of such data in FAFTEEC lies in the fact that it is derived from aircraft engaged in a variety of environments. Users are primarily:

- Air National Guard
- Tactical Air Command
- Navy

DDA used its computerized data retrieval system for reliability data on DDA engine components including control components. Input data from the following sources is screened extensively before acceptance into the system:

- Configuration Life Accounting
- Unit Time Reports
- Modifications
- Overhaul/Repair Input Data
- Failure/Event
- Part Condition
- Material Review Board
- Accident

For FAFTEEC reliability data was retrieved for 12 TF41 control components with 10 years of Fault-information data analyzed (1970-79). Information was sorted within component by:

- Part Number
- Serial Number
- Incident Data
- Operational Part Time
- Primary Reason for Removal

7 of the 12 TF41 components related appropriately to FAFTEEC control components.

Data for the remaining FAFTEEC non-electronic modules came from control vendors, particularly Bendix.

(d) Use of Data

While individual module failures may be derived from these module reliability numbers, the primary goal impacting FAFTEEC designs, the probability of mission completion, depends on the state of the system rather than the state of an individual module. Thus an additional table of information is necessary relating probability of system failure to a particular module failure.

For the FAFTEEC Baseline modules an abort percentage was applied to each module. Each abort percentage is based on identifying the failure mechanisms for each module, and then determining which of these mechanisms would cause system failures. Thus the module abort rates represent the numbers to be used in evaluating the probability for mission completion. The module failure rates are still vital in determining repair events. Note that a module failure which does not cause a system abort may still cause degraded performance, but it is assumed that the degradation will not be severe enough to prohibit mission completion. Also note that abort percentages of zero can infer one of two things in the case of the baseline system:

(1) When associated with a sensed value, the sensed parameter is used for trim only

(2) When associated with an actuator, the item fails safe

(c) Cost Support Data

Cost support data was required to analyze the Life Cycle Cost impact of a fault-tolerant control system.

When modules fail in the FAFTEEC fault-tolerant configurations it was assumed that they could be replaced as line replacable units (LRU). The only exception to this is the digital controller. Since the digital controller actually represents multiple modules in the FAFTEEC baseline system, it was assumed that any module which was a part of the digital control unit would not itself be considered a LRU but rather the digital controller would be considered a LRU.

As an LRU any module may be replaced at various maintenance levels - in the shop (depot), at the base, and on the flight-line (on or off the aircraft). Then, depending on the severity of module failure, the module which is replaced may be repaired at any one of these maintenance levels, or returned to the component manufacturer for repair. All of this information needs to be formatted for use by the reliability and cost models. To accommodate the model forms information was obtained for each of the modules representing:

- the probability of module repair at a given maintenance level
- the cost of material for a repair occurring at each level
- the labor charges (man-hours) to effect repair at each level

This information will not be detailed here, but this information is critical in determining operating expenses. Therefore, conservative maintenance input estimates were used in determining these costs.

SECTION VI
FAULT TOLERANT SYSTEM DESIGN STUDY

The FAFTEEC approach to development of fault-tolerant system configurations was to:

(1) Use the systematic design approach discussed in Section I.

(2) Characterize fault-tolerant control system configurations through the use of component redundancy, various recovery strategies, and different maintenance policies.

(3) Screen those fault-tolerant configurations with an inexpensive reliability evaluation tool.

(4) Select a few attractive configurations from this screening process, and conduct a more detailed reliability and life cycle cost evaluation.

Sections III and IV discussed the establishment of a baseline system definition and the configuration process in step (2) above. Steps (3) and (4), the actual fault-tolerant system analysis procedure, will be discussed in this section. This procedure used the tools discussed in Section V for clarification purposes.

1. FAULT TOLERANT SYSTEM SELECTION

In the initial phase of the reliability analysis a constant failure rate (CFR) modeling procedure was adopted. This approach provided the capability for a systematic synthesis of a large number of redundant architectures. The technique analyzed each fault-tolerant candidate system as a series of functioning modules. The design methodology used Markov models to calculate preliminary costs and mission reliability. Candidates were screened and reliability drivers identified. Module redundancy and varying module maintenance policies were evaluated. Cost and weight factors were used to trade-off alternatives.

(a) Approach

This section illustrates the method for selecting configurations for analysis. At the module level the user of GRAMP could conceivably specify, for a given module, its maintenance level, its redundancy level, and its coverage level(s). In the FAFTEEC analysis 3 module levels were considered for maintenance. Additionally redundancy level was restricted to triplex configurations or less. For each redundancy level a level of coverage definition is required.

Early analysis results indicated the need to consider an additional mission reliability goal. While one set of systems was evaluated with respect to the initial reliability goal, an additional set of configurations was analyzed with respect to a reduced reliability goal of .9995. The initial goal was reduced primarily due to the poor simplex reliability of the actuators. These modules had failure rates in the range of 100 to 500 failures per million hours (FPMH), an order of magnitude higher than the electronics. These constraints severely limited the reliability of the candidate designs and led to the definition of a more realistic and realizable design goal.

Thus, a specific set of design assumptions and constraints were adopted to insure that the proposed system configurations were realistic for the mission reliability goal. These constraints primarily addressed the bounds on coverage and the extent of replication considered reasonable for the hydromechanical modules. The design assumptions included:

- The actuators and torque motors could have no more than duplex hardware redundancy.

- Triplex modules would have coverage less than or equal to .999, .99.

- Duplex modules would have coverage less than or equal to .99.

- o The fuel pump module, fuel module and speed sensors were considered duplex with coverage .99.

- o The coverage on the four torque motors, four resolvers and PMA module was considered nearly perfect because they employ winding replication.

The component data for the non-electric components did not consider that some portion of the component failure modes (e.g. leaks) would not impact successful completion of a mission. Given a successful transfer to backup control, these failures would not impact mission success. Based on available data, an estimate was prepared of the percentage of failures that would result in mission aborts. Module abort rates were derived using the percentage assumption. The abort rates were then used as the failure rate input data for the GRAMP analysis of the candidate configurations.

Component acquisition cost and weight data was configured for proper input to the GRAMP model. This allowed preliminary quantification of relative factors to prioritize alternative designs. A module repair charge of 20% of the module acquisition cost plus the component replication cost provided an input for calculating associated cost figure of merit for each configuration.

These assumptions coupled with the specification and evaluation of desired sensitivities lead to a reasonable number of configurations for CFR anlysis with respect to the reduced mission goal.

The design procedure required the generation and anaysis of a large number of candidate configurations. Each architecture addressed a particular design approach or objective. The final selection required an evaluation to determine which configurations best satisfied the objectives, primarily from the standpoint of reliability and maintainability and secondarily from cost and weight.

(b) Configurations Selected

This process resulted in six configurations. Candidate 1 represented the Baseline system as interpreted by GRAMP. Systems 2 and 3 evaluated the architecture necessary to satisfy the original mission reliability goal of .9999975. Systems 4, 5, and 6 addressed the reduced mission reliability goal (.9995).

Each proposed candidate configuration represents a different design objective. These are listed in Table 14. Case 1, the baseline design, is used as a reference for analyzing the other five configurations. Case 2 investigates the magnitude of the coverage needed for .9999975 reliability, given that the system is maximum hardware redundant with maximum maintenance.

Case 3 examines the extent to which the failure rates would have to be lowered in a maximum hardware, maintenance, and coverage system to meet the 0.9999975 reliability goal.

The remaining three feasible cases are designed to meet the reduced reliability goal of .9995. The objective of Case 4 is to minimize hardware with a maximum maintenance policy. Case 5, on the other hand, attempts to increase the mean time between repair (MTBR) by minimizing the maintenance requirement with a maximum hardware constraint. The final configuration (Case 6) while attempting to maximize MTBR subject to a .9995 reliability, illustrates opportunistic maintenance by modeling groups of electronics modules in the same subsystem and then repairing all the modules when one of them reaches its maintenance level.

This section gives a detailed description of the six candidate configurations and the necessary input: i.e., redundancy, maintenance level, failure rate and coverage used for each case. The cost evaluation model (CEM) and Reliability Feasibility Model (RFM) summary results are given in Table 15.

Table 14. FAFTEEC Candidate Configurations

Case	Objective	Description
Case 1	Baseline	GMA200 System
Case 2	Coverage required for original goal	Triplex all modules Maintenance level 1 (ℓ = 1) Coverage must be .9999, .9999
Case 3	Failure rates required for original goal	Triplex all modules Maintenance level 2 (ℓ = 2) Coverage of .999, .99 Module Failure rates = 10.0
Case 4	Minimize hardware and maximize maintenance	Duplex 3 act, Cov = .99, ℓ = 1 Duplex 4 T.M., Cov = 1.0, ℓ = 1 Duplex databus, Cov = .97, ℓ = 1 Duplex power, Cov = .97, ℓ = 1 Duplex A/D, Cov = .97, ℓ = 1 Duplex CPU, Cov = .97, ℓ = 1 Triplex CCU, Cov = .97, .97, ℓ = 2 Press and Temp A/R
Case 5	Minimize maintenance and maximize hardware	Duplex 3 Act, Cov = .99, ℓ = 1 Duplex 4 T.M., Cov = 1.0, ℓ = 1 Duplex power, Cov = .99, ℓ = 1 Duplex excitation, Cov = .99, ℓ = 1 Triplex CPU, Databus, A/D, Output, CCU, Exiter/Igniter, and Resolvers, Cov = .999, .99, ℓ = -1 Press and Temp A/R
Case 6	Illustrate opportunistic maintenance on electronics to increase MTBR	Duplex 3, Act, Cov = .99, Duplex 4 TM, Cov = 1.0, ℓ = 1 ON 1 T.M. Duplex Databus, Cov = .99, ℓ = 1 Electronics Subsystem Duplex Power, Cov = .99, ℓ = 1 Duplex Output, Cov. = .99, ℓ = -1 Duplex A/D, Cov = .99, ℓ = -1 Duplex CPU, COV = .99, ℓ = -1 Triplex CCU, Cov = .999, .99, ℓ = -1 Duplex Excitation, Cov = .99, ℓ = -1 Press and Temp A/R

Table 15. Constant Failure Rate Results for Candidate System

CASE	TEST CASE OBJECTIVE	RELIABILITY		ABORT RATE (FPMH)	INTERVALS		WEIGHT (LB)
		t=3	t=10		MTBF	MTBR	
CASE 1	BASELINE	.995992	.986701	1339	747	747	285
CASE 2	COVERAGE REQUIRED FOR ORIGINAL GOAL	.9999983	.999989	.33	3,013,470	616	602
CASE 3	FAILURE RATES REQUIRED FOR ORIGINAL GOAL	.9999975	.999992	.83	1,207,760	1,218	602
CASE 4	MINIMIZE HARDWARE AND MAXIMIZE MAINTENANCE	.999532	.998428	155	6,436	455	416
CASE 5	MINIMIZE MAINTENANCE AND MAXIMIZE HARDWARE	.999501	.998324	166	6,028	500	430
CASE 6	ILLUSTRATE OPPORTUNISTIC MAINTENANCE ON ELECTRONICS TO INCREASE MIBR	.999502	.998328	153	6,552	508	417

The baseline system with its 41 modules was evaluated through GRAMP using abort rates in lieu of failure rates for each module. The reliability for this configuration was determined to be .99599 and the MTBR was 747 hours.

Case 2 defined the coverage necessary to meet a .9999975 reliability given that the system has all modules triplex with abort rates and maintenance strategy is to repair when any module fails. The necessary coverage was calculated as .9999, .9999. Deferring the maintenance (i.e. repair when two modules have failed) did not reduce FAFTEEC reliability. Therefore, the case 2 design was to triplex all modules using a coverage of .9999, .9999 and to repair only when two modules had failed (level 1 maintenance).

Given all modules triplex with the coverage constraint of .999, .99 and a maintenance strategy to repair when any module fails, Case 3 investigated the degree to which the failure rates would have to be lowered in order to achieve a reliability of .9999975. GRAMP showed that all modules with abort rates more than 10.0 (FPMH) would have to be lowered to 10.0 (FPMH) to reach the goal.

Cases 4, 5, and 6 were designed to meet the reduced goal of .9995. For these configurations no replication was required in the 7 fail-safe subsystems:

- o nozzle geometry - A8
- o HPT (turbine geometry)
- o nozzle metal temperature
- o memory
- o BLD1 solenoid
- o de-ice
- o backup transfer

Therefore the modules of these subsystems were defined to have zero abort rates. In order to meet the reliability goal in Cases 4, 5, and 6, three actuators (coverage = .99) and four torque motors (coverage = 1) were required to be duplex with repair for any module failure. This was due to the high failure rates of these modules compared to the other 34 modules.

Hardware redundancy and analytical redundancy on the pressure and temperature sensors were compared and evaluated. No reliability improvement resulted from the hardware-redundant design, which is less practical from an engineering design standpoint, more costly and heavier. Therefore, in Cases 4, 5, and 6, a 3-of-4 analytical redundancy scheme was assumed for the pressure sensors. The 1553 databus was used to synthesize T1, T3, or T5 for the temperature sensors.

In Cases 4, 5, and 6, as in the baseline case, the speed sensors, fuel metering, and fuel pump modules are all defined to be duplex with .99 coverage.

The PMA module was modeled with the airframe source (failure rate = 1.0 FPMH) as a single subsystem. If either the PMA or the airframe source were operational, the subsystem was considered to be operational.

Also, in Cases 4, 5, and 6, based on the digital control design, the CCU module was triplex with a maximum coverage of .999, .99 and the CPU module was defined to be at least duplex with a maximum coverage of .99. The memory module design, with its Hamming Error Detecting and Correcting (EDC) codes, was considered equivalent to a simplex fail-safe memory.

The final Cases (4, 5, and 6), which achieve the .9995 reliability goal, are illustrated in Figures 18 through 20. The objective of Case 4 is to minimize hardware with a maximum maintenance poicy while satisfying the .9995 reliability goal. As in the baseline case, the speed sensors, fuel metering and fuel pump modules are all duplex with a .99 coverage. No maintenance is specified for the speed sensor, but maintenance can be performed on the fuel and fuel pump modules. In this case, a maintenance level 1 is used on these two modules to meet the maximum maintenance constraint in the objective. The three actuators are duplex with a .99 coverage objective. The four torque motors

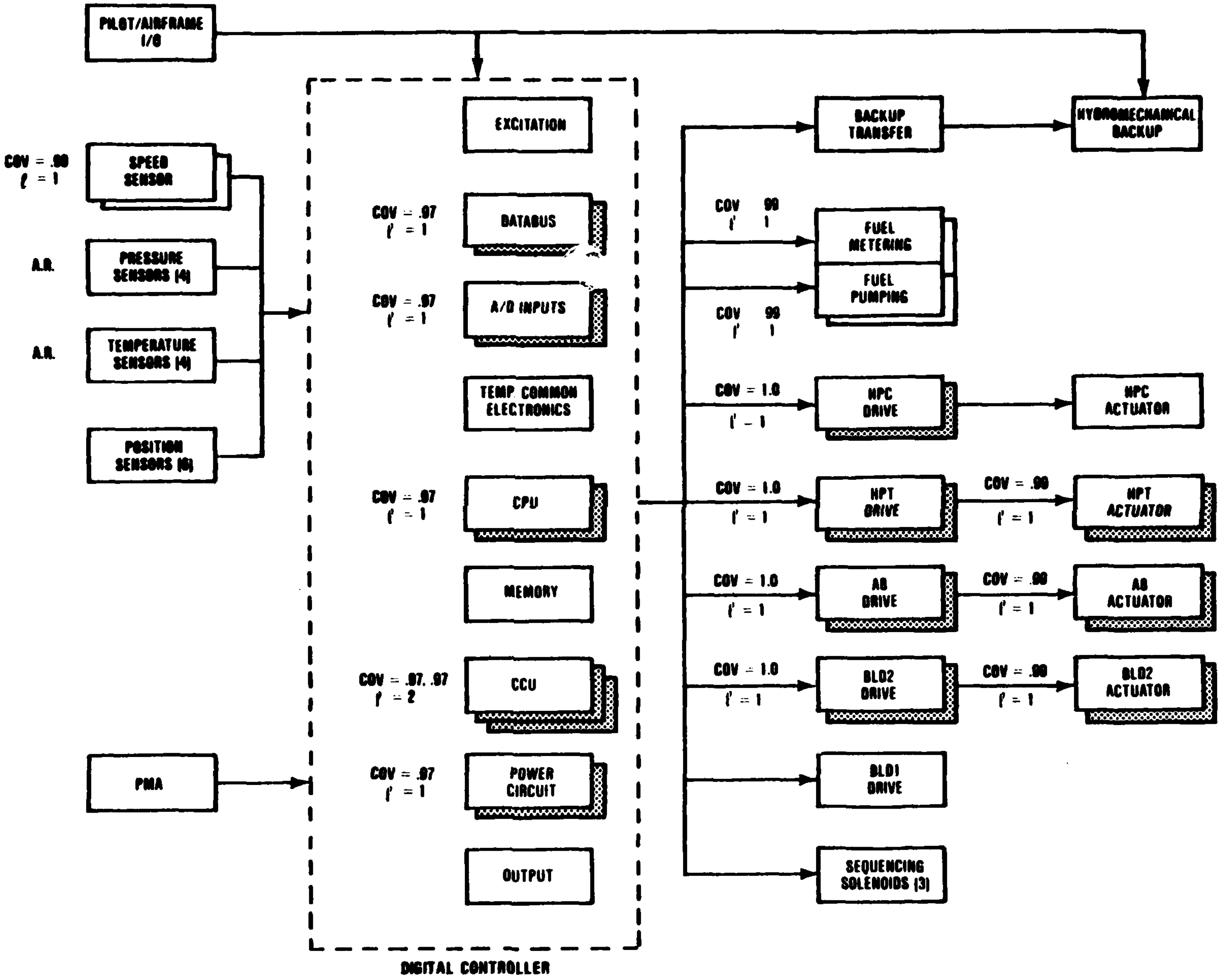


Figure 18. FAFTEEC Derivative Control System - System 4

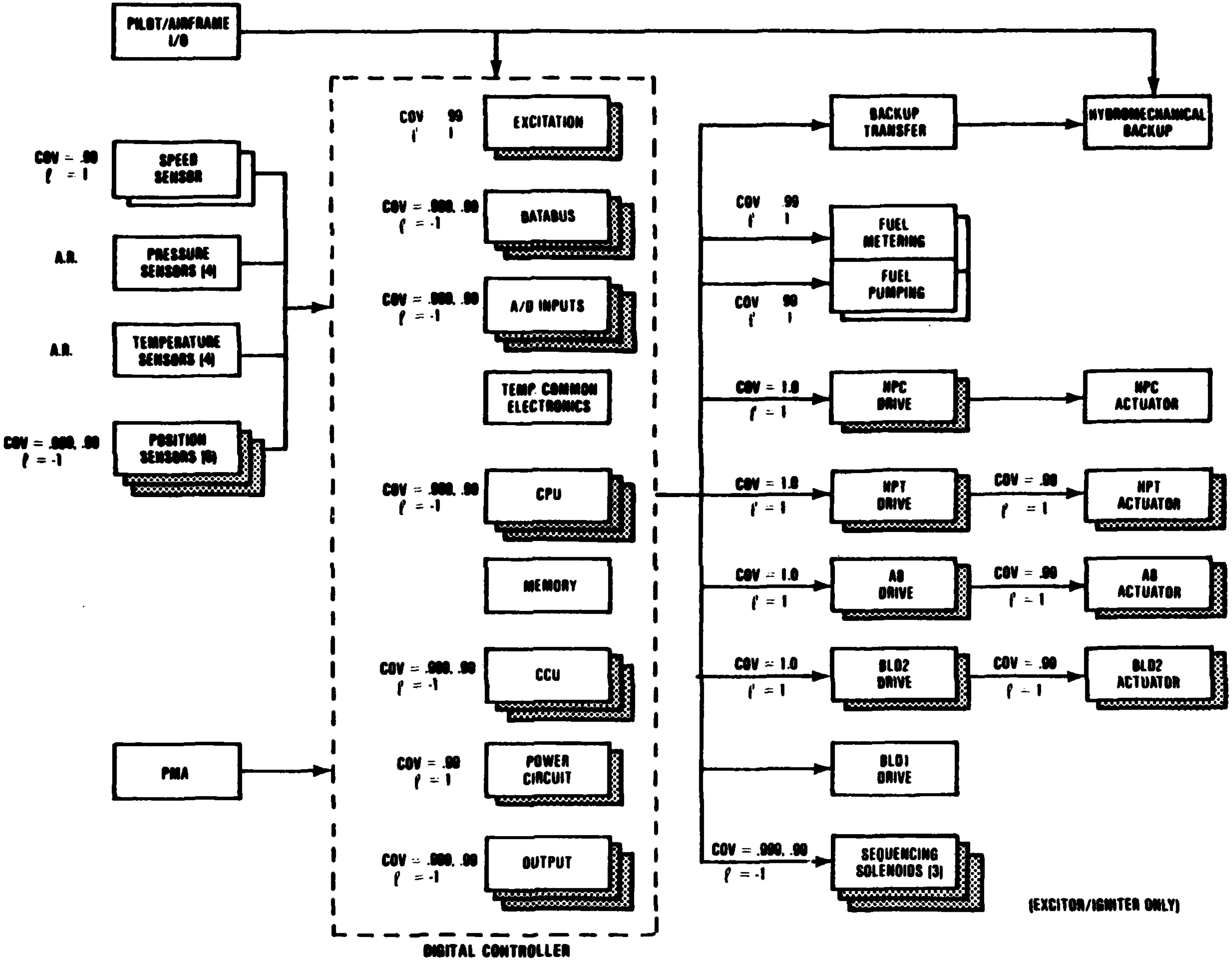


Figure 19. FAFTEEC Derivative Control System - System 5

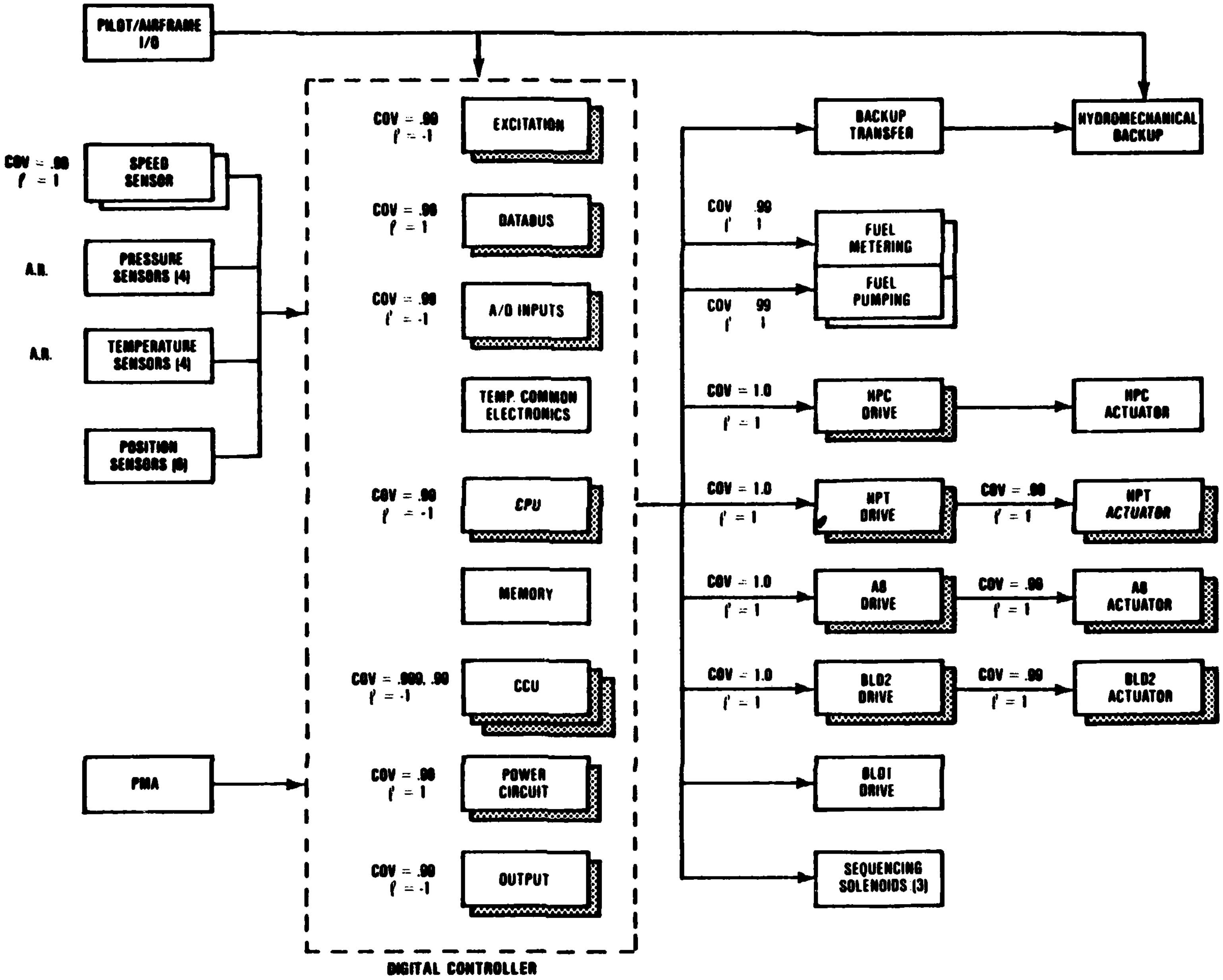


Figure 20. *FAFTEEC Derivative Control System - System 6*

are duplex with perfect coverage and maintenance required if any individual module fails. Analytical redundancy is proposed for the temperature and pressure sensors. In order to meet the goal with minimum hardware, three of the high failure rate electronics modules, in addition to the CPU and CCU definition (maximum maintenance on both), must be duplex. They are the power circuit, 1553 databus, and A/D input modules. The coverage on all five electronics modules can be reduced to .97 (duplex) and .97, .97 (triplex), and still achieve the desired goal.

The objective of Case 5 is to increase the MTBR by minimizing maintenance and maximizing hardware to its feasible capability. The speed sensors, fuel metering and fuel pump modules are all duplex with no maintenance. Analytical redundancy on temperature and pressure sensors is also included in Case 5. The three acutators (coverage = .99) and four torque motors (coverage = 1) are duplex with maintenance if any module fails. In order to achieve the goal of .9995, the power circuit (maintenance specified) and excitation modules (no maintenance) must be duplex with a coverage of .99. The 4 resolvers, databus, A/D inputs, output, CPU and exciter/igniter are all triplex with .999, .99 coverage and no maintenance. From this case, it becomes evident that it is difficult to minimize the necessary maintenance. However, maintenance modeled in GRAMP is specified on a module level, not opportunistically and not with periodic scheduled maintenance. Inclusion of these other maintenance policy options would increase the MTBR.

Case 6 attempts to illustrate opportunistic maintenance by modeling groups of modules in a subsystem and then repairing all failed modules when any one of them reaches its maintenance level. To meet the .9995 reliability goal, the three actuators must still remain duplex with maintenance even when grouped in the same subsystem. If the maintenance on any module in the actuator subsystem is deferred, it is impossible to achieve the goal. However, maintenance must only be performed on one of the high failure rate duplex torque motors (HPT or A8) when they are grouped in the same subsystem. In this configuration, the temperature and pressure sensors are left analytically redundant as specified previously. The databus, now incorporated in the temperature subsystem, must be duplex with .99 coverage. Failure of a databus requires maintenance on this subsystem. The fuel and fuel pump modules form the fuel subsystem and are both duplex. Maintenance need only be specified on the fuel module, not on the fuel pump module. The CCU, CPU, output, A/D input and power circuit modules constitute the electrical subsystem. All but the CCU module are duplex with coverage of .99. The CCU is triplex as defined previously with coverage of .999, .99. Maintenance is done opportunistically on the entire electrical subsystem whenever a failure occurs in the power circuit module. In addition, the excitation module must be duplex with .99 coverage and no maintenance. Invoking this opportunistic maintenance option in GRAMP allows the MTBR to increase to 508 hours from 464 hours (in Case 4) and yet still achieves the .9995 reliability goal. Inclusion of more precise opportunistic and periodic maintenance would increase the MTBR even further.

The Generalized Reliability and Maintainability Program (GRAMP) used to evaluate candidate FAFTEEC configurations does not take into account periodic maintenance or in-depth opportunistic maintenance. These policy strategies are evaluated in the FAFTEEC Monte Carlo simulation and impact both reliability and maintainability.

Five general statements can be made about the FAFTEEC designs.

(1) The three actuators and 4 torque motors must be at least duplex with maintenance and coverage greater than .99.

(2) A 3-of-4 analytical redundancy scheme should be implemented on the pressure sensors.

(3) The temperature sensors must be able to be synthesized with additional data from the 1553 databus.

(4) After the above items are addressed, the power circuits and databus become the electronics reliability drivers for the system.

(5) The incorporation of opportunistic maintenance type policies improves the MTBR and reliability as predicted.

2. FAULT TOLERANT SYSTEM MAINTAINABILITY AND COST ANALYSIS

For the second phase of the analysis the GRAMS model, described in Section V which includes the capability for a time varying analysis, was used as a tool in the final system analysis. This approach provided the capability for detailed analysis of the six candidate architectures discussed earlier in this section. GRAMS was used to calculate reliability, maintainability and life cycle cost contributing factors. The database, sample size determination and evaluation results are discussed in the following sections.

(a) Maintainability and Cost Analysis Approach

Having established 6 candidate configurations, further detailed analysis was conducted through GRAMS (described in Section V). As stated in that section GRAMS analysis was conducted to better characterize the system reliability in the face of:

- o a more detailed maintenance strategy
- o discrete events characterization
- o engine related events

The more detailed maintenance strategy including on-condition maintenance, deferred maintenance, and opportunistic maintenance was included to determine the impact on MTBR. Characterization of discrete events, such as lightning or engine overtemperature liklihood, was included to investigate the effect of these events on mission reliability.

In addition to these items GRAMS possesses the ability to characterize component failure rates nonlinearly (i.e. Weibull, Duane). This was exercised only for the system reliability driver (the air motor actuator). For all other non-electronic components insufficient information existed to properly characterize the wear out phenomena, should one exist. Similarly, although assembly data indicated that components in the digital controller exhibited burn-in aspects (i.e. decreasing failure rates with increasing operating time), this was not used in characterizing the failure rates of the modules in the controller.

The component database, as listed in Appendix B, was utilized to perform the GRAMS analysis. The failure rates and abort rates used in GRAMP were used, for each of the system modules. Each of these modules was defined to be a line replaceable unit (LRU) for the controller.

Every module was assigned the potential to fail because of a maximum temperature or lightning event. Also, certain components were designated to be removed periodically for scheduled maintenance. Maximum operating times (MOT) were assigned for modules. In addition, replacement charge costs in dollars are given for all of the modules.

In addition to module level data, system input data including such items as mission mix, engine service life, engine scheduled and unscheduled removal rates, number of engines in fleet, number of engines to be simulated and system maintenance costs were used by GRAMS and are listed in Table 16, as well as a brief description of each variable.

Using the confidence interval procedure implemented in GRAMS, the sample sizes (N*) required to run the Monte-Carlo simulation were determined. The sample size changes for each variable and it is a function of the tolerance allowed and significance level (a) chosen. Table 17 lists by variable the sample size required for both 95% and 99% confidence given a specific tolerance for System Numbers 1, 2, 3, 4, 5, and 6.

Table 16. GRAMS System Level Inputs

Variable	Description	Value
TLIFE	Hours per engine life	7000
HPY	Hours per year	466.7
DTA	Type A mission length (hours)	3
PDTA	Probability of mission type A	.9
OTB	Type B mission length (hours)	10
DSWNR	Probability of doing end of flight maintenance even when not required	.02
DSWR	Probability of doing end of flight maintenance when required	.98
PMAXT	Number of maximum temperature occurrances per million hours	36539
NSEVB	Number of severity levels for maximum temp.	2
BSEV	Probability for severity each level of max. temperature	.684/.316
PLITE	Number of lightning events per million hours	10.08
NSEVP	Number of severity levels for lightning	1
PSEV	Probability for each severity level of lightning	1
EMOT	Time in hours between scheduled engine removals	1500
EFAIL	Probability of engine failure on any mission	.0160557096
NFLEET	Number of engine in fleet	1000
EPS1	MOT screening interval for installed systems (hours)	10
EPS2	MOT screening interval for uninstalled systems (hours)	225

Table 16 (continued)

Variable	Description	Value
PBUIF	Probability of backup inspection failure	0
PBUSF	Probability of backup switch failure	0
CBUIF	Cost of backup inspection failure	0
CBUSF	Cost of backup switching failure	0
CSLRU	Cost of scheduled flight line maintenance	0
CULRU	Cost of unscheduled flight line maintenance	0
COP	Cost of opportunistic maintenance	1500
CSSH	Cost of scheduled shop visit	0
CUSH	Cost of unscheduled shop visit	0
NSIM	Number of engines	10,000
TFRD	Non-constant failure rate input times	0, 300, 600, 900, 1200, 1500, 1800, 2100, 2400, 2700, 3000, 7000

Table 17. Sample Size Determination for Analysis through GRAMS

System				n*	
Number	Variable	Estimate	Tolerance	95%	99%
1	Reliability (3)	.9964	.0001	852	1,795
	Reliability (10)	.9983	.00005	1,385	2,918
	Abort (FPMH)	1,187	10	7,458	15,712
	MTBF	844	10	3,889	8,193
	O&S cost/hr.	6.98	.1	319	761
2	Reliability (3)	.99995	.00001	1,635	3,456
	Reliability (10)	.99978	.00005	2,003	4,232
	Abort (FPMH)	18.55	1	8,470	17,897
	MTBF	55,747	3,000	9,648	20,386
	O&S cost/hr.	14.03	.1	212	402
3	Reliability (3)	.999945	.00001	1,753	3,328
	Reliability (10)	.999772	.0001	612	1,294
	Abort (FPMH)	55,862	10,000	6,517	12,372
	MTBF				
	O&S cost/hr.	7.87	.1	245	518
4	Reliability (3)	.9993	.0001	243	572
	Reliability (10)	.9976	.0001	8,097	17,109
	Abort (FPMH)	230	10	2,573	5,437
	MTBF	4,250	100	9,056	19,135
	O&S cost/hr.	11.9	.1	311	591
5	Reliability (3)	.9996	.0001	138	293
	Reliability (10)	.9986	.0001	4,494	8,532
	Abort (FPMH)	136	10	639	1,350
	MTBF	7,300	150	8,523	18,010
	O&S cost/hr.	12.2	.1	226	478
6	Reliability (3)	.99935	.0001	153	288
	Reliability (10)	.9977	.0001	5,487	11,593
	Abort (FPMH)	215	10	906	1,913
	MTBF	4,650	100	4,464	9,432
	O&S cost/hr.	12	.1	235	496

Based on the results of this analysis, it was determined that the sample size required was very sensitive to the tolerance chosen. Looking at a range of tolerance levels for all the variables led to the conclusion that 10,000 engines simulated over a 15 year period would be more than adequate. To illustrate, Table 18 shows the confidence in four of the variables after running 10,000 engines in Case. 4.

Table 18. Confidence in GRAMS Results using 10000 Engines

Variable	Estimate	Tolerance	Confidence
Reliability (3)	.9993	.0001	100%
Reliability (10)	.9976	.0001	96%
Abort (FPMH)	230	10	99.8%
MTBF	4,250	100	95.5%

(b) Time Varying Analysis Results

Each of the cases was translated into appropriate redundancy level and maintenance strategy input for GRAMS. Each of the electronic component modules which are part of the actual computer was grouped into one subsystem to improve the reliability through opportunistic type maintenance.

The system results including reliability for 3 & 10 hour missions, system failures (FPMH), mean time between failure (MTBF) and O&S costs per hour ($) are listed in Table 19. Table 20 contains the system mean time between repairs (MTBR) for both shop and LRU unscheduled, scheduled, and opportunistic maintenance.

In comparing the results of the GRAMP versus GRAMS model it was necessary to consider the various maintenance strategies, discrete event and engine related occurrences that are included in the latter model. When both models were run using exactly the same input data, the results were statistically equivalent.

Table 19. Summary of GRAMS Results for Candidate Systems

System	Reliability		System Failure		
Number	t = 3	t = 10	Rate (FPMH)	MTBF	O&S/hr.
1	.9960135	.9868505	1,325	755	7.38
2	.9999873	.9999465	4.5		15.7
3	.9998934	.9996614	35	28,513	19.13
4	.9996102	.9986415	131	7,605	12.85
5	.9998769	.9995801	41	24,230	13.65
6	.9997249	.9990858	92	10,917	13.00

Table 20. Summary of MTBR's for Candidate Systems

System	Scheduled		Unscheduled		
Number	LRU	Shop	LRU	Shop	Opportunistic
1	6,374	20,846	795	187	1,254
2	5,248	19,915	995	189	976
3	3,141	28,340	320	190	807
4	4,201	23,156	470	189	918
5	4,281	23,011	543	189	847
6	4,261	22,457	531	189	855

However, in using the input data it became evident that the results would not be equivalent. The results of the Monte Carlo simulation GRAMS which included a 3 and 10 hour mission mix showed that relative to the GRAMP CFR analysis the inclusion of maximum temperature and lightning events decreased the system reliability slightly. However, four factors increased the overall reliability in the fourth decimal place from .9995 to a range of .9996 and .9998. The first factor was combining all the electronics modules into one subsystem thereby allowing for LRU opportunistic maintenance on the controller using an adequate diagnostic system for repair determination. The second factor was the inclusion of scheduled component maintenance. Component MOT's cause items to be repaired before failure resulting in increased reliability; likewise for the third factor which was engine scheduled shop visit or MOT within a certain specified screening interval. The fourth factor, also engine related, was an unscheduled engine removal due to some failure. The third and fourth factors just described force the engine host and fault-tolerant control system into the shop for repair. At this point, engine driven opportunistic maintenance on failed redundant components occurred causing the majority of the increase in system reliability.

The mean time between repair (MTBR) goal of 1800 hours was in actuality achievable if it was considered to include only unscheduled repairs (MTBUR). However, in the GRAMP CFR analysis, MTBR includes preventative and deferred maintenance. But the mean time between failure (MTBF) values were calculated based on a failure that caused an unscheduled removal and therefore an unscheduled repair. For the achievable cases 4, 5 and 6 this value was equivalent to a MTBR value of greater than 6000 hours, surpassing the 1800 hour goal.

In the GRAMS final system evaluation results, engine related as well as FAFTEEC related repair and maintenance events were included. Therefore, the results as presented in Table 19 were broken out into mean time between various maintenance levels. Again, maximum temperature, lightning and engine driven occurrences led to the various MTBR values.

Output from the final system evaluation relative to the redundant system configurations was interfaced with the life cycle cost analysis procedure to compute total cost of ownership.

3. FAULT-TOLERANT SYSTEM LIFE CYCLE COST DETERMINATION

Although GRAMS provided a detailed maintenance strategy with associated repair charges, additional work was required to arrive at the true life cycle costs (LCC) associated with a given system. These include not only the Operating and Support costs resulting from maintenance, but also design related expenses (RDT&E), and new system and component replacement charges (Acquisition).

(a) Life Cycle Cost Analysis Procedure

Life Cycle Costs were calculated for 4 systems previously described - the baseline and cases 4, 5, and 6. For each case module information representing development costs and unit acquisition cost were usefu' in computing LCC.

The RDT&E charges associated with a particular system design were calculated as the sum of each modules RDT&E cost. The cost for each module, obtained from Appendix A for the Baseline system, is assumed to include not only the costs associated with that particular component's development but also the integration costs associated with that component.

The difference between system RDT&E costs, when associated with fault-tolerant systems such as in FAFTEEC, is impacted by such effects as:

- o System integration costs associated with redundant configurations
- o Fault recovery strategy costs associated with redundant configurations

Since all configurations are made up of various redundant levels of identical modules, these costs represent the chief differences in RDT&E charges in the FAFTEEC analysis.

The LCC procedure used GRAMS output summaries for 2 sources of information:

- o Direct calculation of Operating and Support Costs

- o Indirect calculation of Acquisition costs associated with investment spares

The GRAMS model outputs Operating and Support Cost rates directly as was shown in the column of Table 19. For each of the four configurations the respective O&S rate was multiplied by the number of engine operating hours for the fleet over a given time period.

Another GRAMS' output, the number of maintenance events per module, yielded information necessary for calculating one of the Acquisition cost contributors, that for investment spares. The number of investment spares was determined for each configuration to provide a two year replacement supply for each module spread throughout the selected number of maintenance facilities. In the case of those modules which had very low failure rates, spares were inventoried such that at least one module per maintenance facility was allocated.

The major Acquisition element in LCC for FAFTEEC was the initial investment cost for equipping all engines in the fleet with control systems.

An additional LCC consideration, the effect of added control system weight for fault-tolerant structures, was also evaluated. In FAFTEEC a penalty charge per added pound of control system weight was calculated and attribted to Aircraft related Acquisition cost.

(b) Life Cycle Cost Results

Table 21 shows the definition of parameters used in the LCC analysis. The first five entries, active aircraft, spare engines (period of operation), engine operating time per month and engine durability define the host (engine) parameters of interest. The items referring to number of bases, number of overhaul facilities, and control modules relate to the maintenance philosophy.

Table 21.

O&S Simulation Boundary Conditions

ACTIVE AIRCRAFT	750
SPARE ENGINES	250
PERIOD OF OPERATION (YEARS)	15
ENGINE OPERATING TIME PER MONTH (HRS)	39
ENGINE DURABILITY	
MAXIMUM OPERATING TIME (HRS)	1500
PREMATURE REMOVAL RATE (PER 1,000 HRS)	4
NUMBER OF BASES	12
NUMBER OF OVERHAUL FACILITIES	1
CONTROL MODULES	LRU
AIRCRAFT ACQUISITION ($/LB/ENGINE)	332
FUEL VARIANCE FROM BASELINE	NONE
ECONOMIC FACTORS	FIXED
ECONOMIC REFERENCE	1981

Table 22

Summary of Life Cycle Cost Results

COSTS IN $M

	CONFIGURATION			
	1	4	5	6
RDT&E	37.35	43.38	44.50	43.38
ACQUISITION				
• INITIAL BUY	171.85	278.40	302.76	281.90
• INVESTMENT SPARES	46.37	84.76	85.76	84.83
• AIRCRAFT RELATED (ABOVE BASELINE)	0	76.63	84.82	77.22
OPERATIONS & SUPPORT	51.66	89.95	95.55	91.00
TOTAL	307.23	573.12 (496.49)	613.39 (528.57)	578.33 (501.11)

The aircraft acquisition penalty charge for additional control weight (above a given reference value) is also defined. Note that no fuel usage related charges are considered within the FAFTEEC LCC analysis. The remaining two entries denote the economic assumptions made in the LCC analysis.

From this input and the pertinent module information the LCC calculations were done on each system. Table 22 shows the results of that anlaysis.

Note that charges related to Acquisition dominated the LCC analysis (≈ 75% of total LCC). This is obviously a function of the cost of a single control system and the fleet size considered. The O&S charges are generally twice that of the RDT&E charges for the fault-tolerant systems but still minimal (≈ 15% of total LCC) with respect to total Acquisition charges.

All three fault-tolerant systems show that by accomplishing the same functional tasks as the Baseline system but improving the Baselines' reliability, an LCC factor increase of approximately two is required. This factor shows the cost penalty associated with achieving a single order of magnitude improvement in reliability beyond a current system.

Note that RDT&E charges do not significantly increase for achieving fault-tolerant structures. This is primarily due to the FAFTEEC procedure for achieving fault tolerance, through redundancy with existing parts rather than parts improvement. Note also that RDT&E charges account for less than 10% of the total LCC for the fault-tolerant configurations. This shows the desirability, from an LCC standpoint, of investing at the RDT&E stage. Such an investment would be attractive for the Baseline system considered, in that resulting Acquisition and O&S charges could be realized.

The O&S charges nearly double for fault-tolerant configurations compared to the Baseline. It is not obvious why this occurs since the fault-tolerant structures were configured to improve system reliability. The increase in O&S costs directly relate to the increased number of components for the fault-tolerant systems considered coupled with the maintenance strategies involved. Thus an increased number of maintenance actions, not necessarily tied to mission criticality but rather convenience, drives the O&S costs.

It should also be noted that one Baseline component, the air motor used in three Baseline modules, is the reliability driver of the system. Being one of the heavier and more costly items in the Baseline, this obviously drives the Acquisition costs. Thus the RDT&E/Acquisition/O&S percentage contributions to LCC could shift drastically by replacing this component.

SECTION VII
CONCLUSIONS AND RECOMMENDATIONS

From the Full-Authority Fault-Tolerant Electronic Engine Control program has evolved a methodology for design of a digital control system with flight safety and system availability as the prime design drivers. The methodology has relied heavily on these analysis tools designated herein as the Generalized Reliability and Maintainability Program (GRAMP), and the Generalized Reliability and Maintainability Simulator (GRAMS), and the Life Cycle Cost (LCC) analysis procedure. These tools were used to develop realistic fault-tolerant control system configurations based on a present VCE control system design.

This systematic model-aided approach was vital in the reduction from a large number of candidate "fault-tolerant" system configurations, based on an existing control system design, to a few derivative systems which actually satisfied a set of prescribed system effectiveness goals and constraints.

GRAMP was the tool most useful in identifying the pneumatic actuation system as the reliability drivers of the FAFTEEC Baseline system. Using this same modular approach the power circuit and databus were identified as the electronic reliability drivers. This implies that system reliability improvements can be made only if these components are addressed through redundancy or other fault-tolerant measures.

Having identified these reliability drivers GRAMP identified a subset of modules for which duplication was mandatory to approach even an oroer of magnitude improvement in reliability or which were needed for safety of flight reasons. Redundancy of the 3 air motor actuators, the 4 torque motors, the speed sensor, the pressure sensors, the temperature sensors, and the fuel pumping/metering system composed this subset.

Finally GRAMP did evolve control system configurations meeting two reliability standards - (1) an order of magnitude improvement beyond present systems, and

(2) an ultimate reliability goal. GRAMP demonstrated that the systems aimed at the ultimate goal required either piece part improvement beyond present technology or fault recovery mechanisms beyond what is presently deemed achievable. GRAMP identified display "candidate" system configurations which met all design criteria with respect to the order of magnitude reliability improvement.

Scrutiny of these "candidates" showed the need to reduce full replication of the costly and heavy hydromechanical components. Analytical redundancy was introduced for temperature and pressure indications to avoid the expense and weight of added sensors. In addition to the replication issue a need to identify/accommodate failure mechanisms consistant with the coverage values required was also exhibited.

On the electronics side an alternative to full scale duplication was presented within the selected replication examples of the "candidates". The necessity for hardware replication and hardware coverage for the digital controller was also evident to contain an insane processor and to achieve the necessary coverage values, respectively.

GRAMS, evaluating the alternate maintenance strategies possible due to a fault-tolerant system structure, showed the desirability of making a control component a line replacable unit (LRU) and thus "moving maintenance toward the flight line". This was due to the lower labor rates associated with repair at the flight line versus those at the base of the depot.

GRAMS also exhibited the importance of stipulating the proper maximum operating time (MOT) on a component exhibiting a wear out characteristic. Removing an item too soon implies less unscheduled repairs and thus a greater mean time between unscheduled repair (MTBUR), but it also implies more maintenance events and, therefore, more operating and support (O&S) costs.

Further, GRAMS showed that engine driven maintenance (opportunistic) could be used to improve reliability, but consequent losses in mean time between repair (MTBR) were experienced.

The LCC analysis showed the Research, Development, Test, and Engineering (RDT&E) charges to be minimal with respect to either Acquisition or O&S charges. Thus parts improvement through slightly increased RDT&E may represent an appropriate investment for fault-tolerant system configurations.

As pointed out in GRAMP, redundancy implies additional components and additional component costs. Thus again in the LCC analysis the system Acquisition costs associated with initial investment reflect the large expense associated with replication of parts. Since this item (initial system acquisition costs) is the cost driver in LCC, this more than ever points toward the need for achieving redundancy with judicious selection of hardware replication.

The investment spares issue was also analyzed for the FAFTEEC candidate configurations during the LCC analysis. This analysis showed that those maintenance strategies involving more maintenance actions would obviously require a greater number of spares to be on hand. This effect could be minimized somewhat by intelligent inventorying of the spares such as placing the majority of the spares at the depot level when imposing an opportunistic maintenance strategy (repair of control when engine requires repair).

The inventorying issue should be carefully considered when addressing the issue of redundancy and distribution of redundancy. Thus a dual configuration consisting of two single strand units may allow less expensive inventorying than use of a dual unit.

The most important conclusion to be made from the LCC analysis, and furthermore for the entire FAFTEEC program, was that significant cost and weight increases could be expected to accompany attainment of improved reliability. For the FAFTEEC Baseline case in point improving the reliability by an order of magnitude implied doubling of the control related life cycle costs over a 15 year time period. Additionally a weight increase of as much as 40% served to penalize such a design due to increased aircraft needs such as added support weight and additional fuel necessary.

These figures merely point to the fact that specification of propulsion control system reliability should be done carefully. Safety of flight considerations are important but achieving these with new maintenance plans and less hardware replication may be cost effective.

In summary the FAFTEEC program has shown the ability to design a "fault-tolerant" control system capable of achieving an order of magnitude improvement in reliability over what can be achieved with present systems. FAFTEEC, in addition to providing a design methodology, has provided a framework for guiding individual control component activities.

APPENDIX A

FAFTEEC DIGITAL CONTROLLER DESIGN

A significant effort was spent during the program in Technology Transfer, transferring information between team members and transferring other industry approaches to fault-tolerant electronics to an electronic engine controller application. This was particularly helpful in design of a fault tolerant digital control architecture. Thus the Design Methodology Approach, as represented in Figure A-1, was coupled with technology transfer from the telecommunication industry for design of the digital controller.

The digital controller is a replacement type redundant system having switchable replacement elements for each functional module. A configuration control unit (CCU) is provided whose primary functions are to accumulate fault status from all digital controller modules, switch in replacement modules where available, and to transfer control to the back-up hydromechanical controller upon detection of a faulty module whose replacements have been exhausted. The CCU is failsafe. A hardware self-checking approach has been adopted which provides near one hundred percent coverage for the critical CPU/Main Memory/Main Bus ensemble. Software checking is used for input, output, analog to digital converter and power conditioning. A simplified block diagram of the digital controller is shown in Figure A-2. The main bus has sixteen data bits plus parity and provides communication between digital inputs, outputs, memory and the central processing unit (CPU). Main bus address and control lines are not shown. However, sixteen address bits plus parity are provided to address the 24K 1K = 1024) read only memory (ROM) locations, the 1K random access memory (RAM) locations, the MIL-STD-1553A data bus, the input analog/digital converter, and the outputs. The CPU is mechanized as a self-checking pair of sixteen bit microprocessors along with the required supporting circuits. The analog to digital converter provides twelve bit digital inputs to the CPU. Each analog output has a dedicated eight bit digital to analog converter along with the required drivers. The power conditioning circuitry converts alternating current power to direct current sources for the digital electronics.

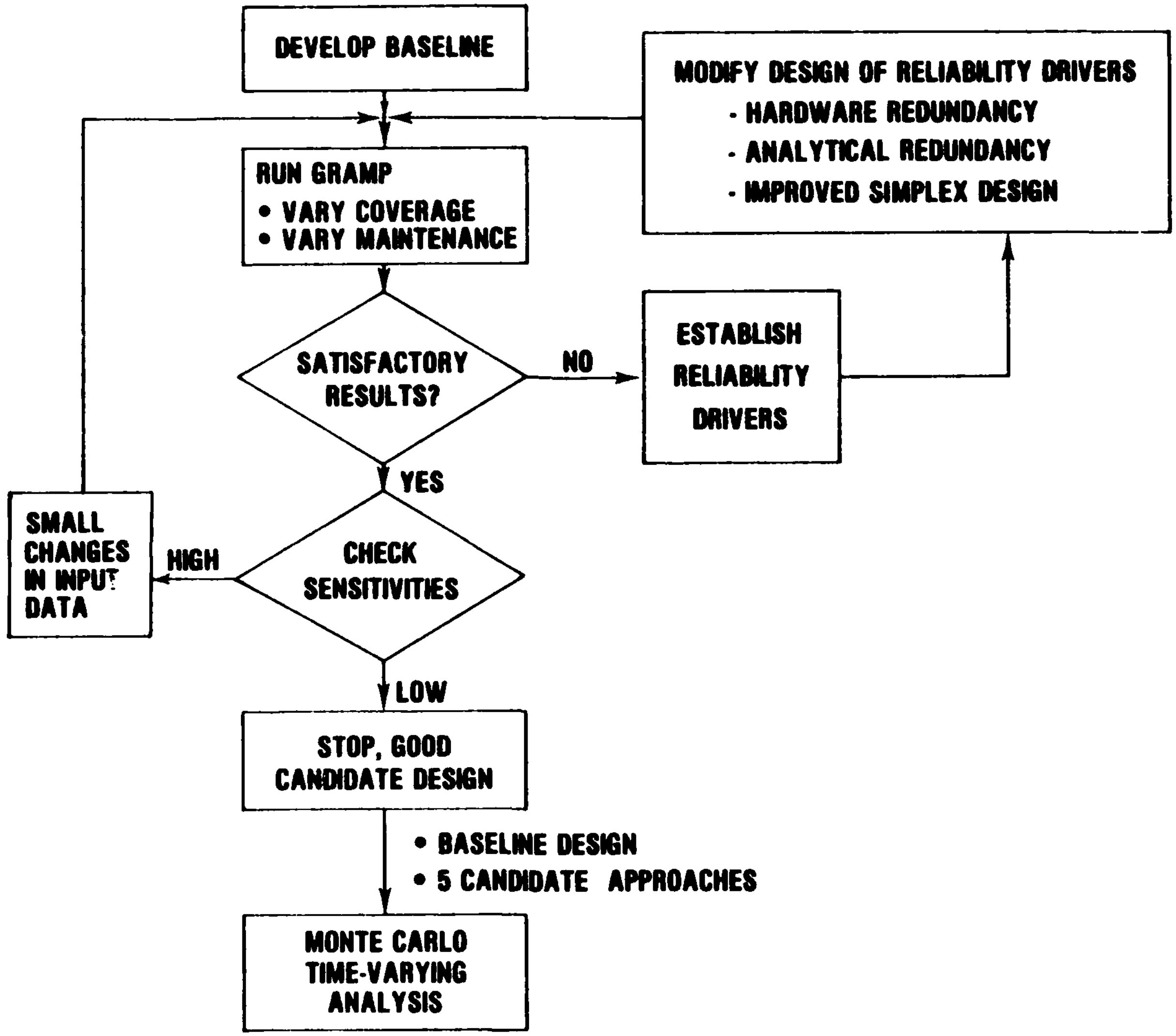


Figure A-1 FAFTEEC System Design Methodolody

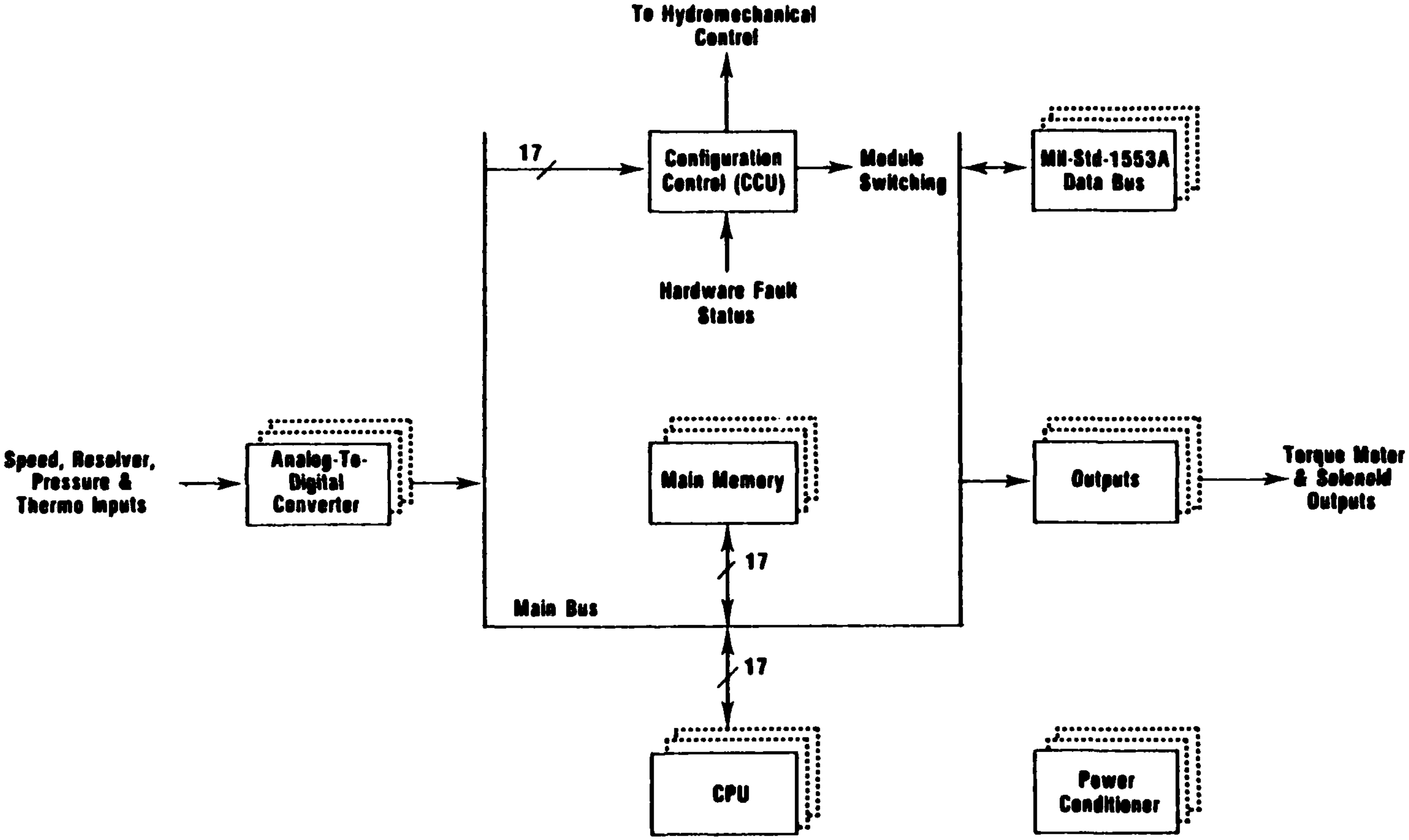

To Hydromechanical Control
17
Configuration Control (CCU)
Module Switching
Mil-Std-1553A Data Bus
Hardware Fault Status
Speed, Resolver, Pressure & Thermo Inputs
Analog-To-Digital Converter
Main Memory
Outputs
Torque Motor & Solenoid Outputs
17
Main Bus
17
CPU
Power Conditioner

Figure A-2 FAFTEEC Digital Controller

Each of the CPU, main memory, analog to digital converter, digital and analog outputs, MIL-STD-1553A data bus and power conditioner modules may be provided with one or more replacement modules. Control signals on the main bus are logically complemented pairs of digital signals (two-rail logic). These main bus signals are checked by the CCU which has the responsibility of monitoring fault status for each of the replacement modules and switching to a good module when one fails. Each of the replacement modules including the power conditioner transmits a two-rail fault status pair to the CCU. A 16 bit data path is provided from the main bus to the CCU for reporting CPU program detected faults.

In the event of a bus fault, a program detected fault, or a hardware detected fault, the CCU switches the appropriate replacement modules. Before switching replacement modules, two actions are initiated by the CCU. FIrst, the CPU is forced to a benign state via a CPU fault trap. Second, a hardened transient timer is started which has a 50-millisecond timeout. This time period is selected for consistency with the maximum allowable controller recovery time of 250 milliseconds and the expected duration of lightning transients. At the completion of the 50 millisecond time interval, the CPU is restarted via an interrupt. A complete restart is used rather than a program rollback since the allowable recovery time is much greater than the expected lightning transient duration.

The CPU modules, main memory modules, and main bus are designed to be totally hardware self-checking; coverage - 1.0. The analog to digital converter, the digital and analog outputs, the MIL-STD-1553A data bus and the power conditioner modules contain partially self-checking hardware for generating two-rail fault signals. Additional software detected faults for these modules are reported to the CCU via the program. The choice of totally self-checking hardware for the CPU/memory/bus ensemble is based on the intuitive notion that a single bit fault in one of these three critical units can give rise to "insane" action in a seemingly unrelated controller output. Furthermore, programmed checks such as end-around analog-digital-analog checks rely on the basic "sanity" of the CPU/memory/bus ensemble. The CCU is mechanized as a triple modular redundant (TMR) module such that single faults are masked. A fault in the CCU causes an immediate switch to the back-up hydromechanical control. The mechanical interface to the hydromechanical control is fail-safe.

Replacement module switching is implemented by providing logical disconnections from the bus for each module's drivers under CCU control. The main bus is not replicated because its failure rate (including drivers and receivers) is relatively low. Bus control logic is clocked rather than asynchronous. The clock generator is duplicated for use throughout the controller. Clock detectors for missing clocks are provided on each module connected to the main bus.

Main memory uses a Hamming code for correction of all single bit data errors and detection of all double bit data errors in a memory word. A total of 25K, sixteen bit words of main memory are required. For coding efficiency, these are organized as 12.5K, 39 bit memory words including 32 data bits and seven Hamming code parity bits for each word.

Two candidate configurations were considered for the CPU replacement element. Both are self-checking and microprocessor based. One configuration, not yet commercially available, is a single internally self-checked VLSI microprocessor. The selected configuration is an externally checked pair of commercially available microprocessors which are run in synchronism, with external comparison circuitry for fault detection. The microprocessor pair is replaced when a noncompare is detected by the external circuitry. The functions of the external circuitry are: 1) Compare two microprocessor outputs for disagreement; 2) parity encode the microprocessor outputs for main bus transmission; 3) check data parity inputs from the main bus; 4) encode two-rail control signal outputs; 5) check two-rail encoded control signal inputs; 6) trap the microprocessors to a benign state upon receipt of a fault trap input from the CCU; 7) restart the microprocessors upon receipt of a restart interrupt from the CCU; and 8) disable the microprocessor pair in response to module switching control signals from the CCU. The external circuitry is mechanized with totally self-checking (TSC) logic such that internal circuit faults are detected.

APPENDIX B

FAFTEEC COMPONENT INFORMATION

FAFTEEC Module: Excitation (Digital Controller)

Module Information Used by GRAMP

Constant Failure Rate	Abort Rate	Unit Cost	Unit Weight
5.8	5.8	500	1.2

Module Information Used by GRAMS

Nonconstant Failure Rate (if appropriate)	Max. Operating Time	Unit Cost	Unit Weight
-	-	500	1.2

		Typical Repair		
Category	At Depot	At Base	At Flightline	On Aircraft
%	100	-	-	-
$	100	0	0	0
MH	4	0	0	0

Probability of Overtemperature Effect		Probability of Lightning Effect
Level 1	Level 2	
-	-	-

Module Information Used by LCC

RDT&E Part of Digital Controller

FAFTEEC Module: Databus (Digital Controller)

Module Information Used by GRAMP

Constant Failure Rate	Abort Rate	Unit Cost	Unit Weight
40.4	40.4	6000	1.5

Module Information Used by GRAMS

Nonconstant Failure Rate (if appropriate)	Max. Operating Time	Unit Cost	Unit Weight
-	-	6000	1.5

		Typical Repair		
Category	At Depot	At Base	At Flightline	On Aircraft
%	100	-	-	-
$	1200	0	0	0
MH	16	0	0	0

Probability of Overtemperature Effect		Probability of Lightning Effect
Level 1	Level 2	
-	-	-

Module Information Used by LCC

RDT&E Part of Digital Controller

FAFTEEC Module: A/D Inputs (Digital Controller)

Module Information Used by GRAMP

Constant Failure Rate	Abort Rate	Unit Cost	Unit Weight
25.2	25.2	3000	1.2

Module Information Used by GRAMS

Nonconstant Failure Rate (if appropriate)	Max. Operating Time	Unit Cost	Unit Weight
-	-	3000	1.2

		Typical Repair		
Category	At Depot	At Base	At Flightline	On Aircraft
%	100	-	-	-
$	600	0	0	0
MH	16	0	0	0

Probability of Overtemperature Effect		Probability of
Level 1	Level 2	Lightning Effect
-	-	-

Module Information Used by LCC

RDT&E Part of Digital Controller

FAFTEEC Module: Temperature Common Electronics (Digital Controller)

Module Information Used by GRAMP

Constant Failure Rate	Abort Rate	Unit Cost	Unit Weight
3.7	3.7	1500	1.2

Module Information Used by GRAMS

Nonconstant Failure Rate (if appropriate)	Max. Operating Time	Unit Cost	Unit Weight
-	-	1500	1.2

		Typical Repair		
Category	At Depot	At Base	At Flightline	On Aircraft
%	100	-	-	-
$	300	0	0	0
MH	8	0	0	0

Probability of Overtemperature Effect		Probability of
Level 1	Level 2	Lightning Effect
-	-	-

Module Information Used by LCC

RDT&E Part of Digital Controller

FAFTEEC Module: CPU (Digital Controller)

Module Information Used by GRAMP

Constant Failure Rate	Abort Rate	Unit Cost	Unit Weight
4.6	4.6	6000	1.0

Module Information Used by GRAMS

Nonconstant Failure Rate (if appropriate)	Max. Operating Time	Unit Cost	Unit Weight
-	-	6000	1.0

		Typical Repair		
Category	At Depot	At Base	At Flightline	On Aircraft
%	100	-	-	-
$	1200	0	0	0
MH	40	0	0	0

Probability of Overtemperature Effect		Probability of
Level 1	Level 2	Lightning Effect
-	-	-

Module Information Used by LCC

RDT&E Part of Digital Controller

FAFTEEC Module: Memory (Digital Controller)

Module Information Used by GRAMP

Constant Failure Rate	Abort Rate	Unit Cost	Unit Weight
0.0	0	9000	1.5

Module Information Used by GRAMS

Nonconstant Failure Rate (if appropriate)	Max. Operating Time	Unit Cost	Unit Weight
-	-	9000	1.5

		Typical Repair		
Category	At Depot	At Base	At Flightline	On Aircraft
%	100	-	-	-
$	1800	0	0	0
MH	40	0	0	0

Probability of Overtemperature Effect		Probability of
Level 1	Level 2	Lightning Effect
-	-	-

Module Information Used by LCC

RDT&E Part of Digital Controller

FAFTEEC Module: CCU (Digital Controller)

Module Information Used by GRAMP

Constant Failure Rate	Abort Rate	Unit Cost	Unit Weight
4.0	4.0	3000	1.2

Module Information Used by GRAMS

Nonconstant Failure Rate (if appropriate)	Max. Operating Time	Unit Cost	Unit Weight
-	-	3000	1.2

		Typical Repair		
Category	At Depot	At Base	At Flightline	On Aircraft
%	100	-	-	-
$	600	0	0	0
MH	24	0	0	0

Probability of Overtemperature Effect		Probability of
Level 1	Level 2	Lightning Effect
-	-	-

Module Information Used by LCC

RDT&E Part of Digital Controller

FAFTEEC Module: Power Circuit (Digital Controller)

Module Information Used by GRAMP

Constant Failure Rate	Abort Rate	Unit Cost	Unit Weight
56.4	56.4	3000	6.5

Module Information Used by GRAMS

Nonconstant Failure Rate (if appropriate)	Max. Operating Time	Unit Cost	Unit Weight
-	-	3000	6.5

		Typical Repair		
Category	At Depot	At Base	At Flightline	On Aircraft
%	100	-	-	-
$	400	0	0	0
MH	24	0	0	0

Probability of Overtemperature Effect		Probability of
Level 1	Level 2	Lightning Effect
-	-	-

Module Information Used by LCC

RDT&E Part of Digital Controller

FAFTEEC Module: Output (Digital Controller)

Module Information Used by GRAMP

Constant Failure Rate	Abort Rate	Unit Cost	Unit Weight
39.1	39.1	3000	1.5

Module Information Used by GRAMS

Nonconstant Failure Rate (if appropriate)	Max. Operating Time	Unit Cost	Unit Weight
-	-	3000	1.5

		Typical Repair		
Category	At Depot	At Base	At Flightline	On Aircraft
%	100	-	-	-
$	600	0	0	0
MH	16	0	0	0

Probability of Overtemperature Effect		Probability of
Level 1	Level 2	Lightning Effect
-	-	-

Module Information Used by LCC

RDT&E Part of Digital Controller

FAFTEEC Module: Fuel Metering

Module Information Used by GRAMP

Constant Failure Rate	Abort Rate	Unit Cost	Unit Weight
86.8	29.5	3180	7.8

Module Information Used by GRAMS

Nonconstant Failure Rate (if appropriate)	Max. Operating Time	Unit Cost	Unit Weight
-	-	3180	7.8

		Typical Repair		
Category	At Depot	At Base	At Flightline	On Aircraft
%	70	25	0	5
$	600	100	0	0
MH	24	4	0	4

Probability of Overtemperature Effect		Probability of
Level 1	Level 2	Lightning Effect
-	-	.001

Module Information Used by LCC

RDT&E $1.125 M

FAFTEEC Module: Fuel Pumping

Module Information Used by GRAMP

Constant Failure Rate	Abort Rate	Unit Cost	Unit Weight
33.1	3.2	5000	12.0

Module Information Used by GRAMS

Nonconstant Failure Rate (if appropriate)	Max. Operating Time	Unit Cost	Unit Weight
-	3000	5000	12.0

		Typical Repair		
Category	At Depot	At Base	At Flightline	On Aircraft
%	95	0	0	5
$	1000	0	0	0
MH	40	0	0	4

Probability of Overtemperature Effect		Probability of
Level 1	Level 2	Lightning Effect
-	-	-

Module Information Used by LCC

RDT&E	$2.5 M

FAFTEEC Module: HPT Drive

Module Information Used by GRAMP

Constant Failure Rate	Abort Rate	Unit Cost	Unit Weight
39.9	39.9	2250	2.1

Module Information Used by GRAMS

Nonconstant Failure Rate (if appropriate)	Max. Operating Time	Unit Cost	Unit Weight
-	-	2250	2.1

		Typical Repair		
Category	At Depot	At Base	At Flightline	On Aircraft
%	100	-	-	-
$	450	0	0	0
MH	16	0	0	0

Probability of Overtemperature Effect		Probability of
Level 1	Level 2	Lightning Effect
.0001	.001	.001

Module Information Used by LCC

RDT&E	$.125 M

FAFTEEC Module: HPT Actuator

Module Information Used by GRAMP

Constant Failure Rate	Abort Rate	Unit Cost	Unit Weight
500	250	20000	26.0

Module Information Used by GRAMS

Nonconstant Failure Rate (if appropriate)	Max. Operating Time	Unit Cost	Unit Weight
Weibull: = 1577 = 2.05	1500	20000	26.0

		Typical Repair		
Category	At Depot	At Base	At Flightline	On Aircraft
%	95	0	0	5
$	2000	0	0	0
MH	40	0	0	4

Probability of Overtemperature Effect		Probability of
Level 1	Level 2	Lightning Effect
.0001	.001	-

Module Information Used by LCC

RDT&E $2.0 M

FAFTEEC Module: HPC Drive Circuit

Module Information Used by GRAMP

Constant Failure Rate	Abort Rate	Unit Cost	Unit Weight
38.6	19.3	2125	2.1

Module Information Used by GRAMS

Nonconstant Failure Rate (if appropriate)	Max. Operating Time	Unit Cost	Unit Weight
-	-	2125	2.1

		Typical Repair		
Category	At Depot	At Base	At Flightline	On Aircraft
%	100	-	-	-
$	450	0	0	0
MH	16	0	0	0

Probability of Overtemperature Effect		Probability of
Level 1	Level 2	Lightning Effect
-	-	.001

Module Information Used by LCC

RDT&E $.125 M

FAFTEEC Module: HPC Actuator

Module Information Used by GRAMP

Constant Failure Rate	Abort Rate	Unit Cost	Unit Weight
13.0	.3	16000	15.0

Module Information Used by GRAMS

Nonconstant Failure Rate (if appropriate)	Max. Operating Time	Unit Cost	Unit Weight
-	-	16000	15.0

		Typical Repair		
Category	At Depot	At Base	At Flightline	On Aircraft
%	10	0	0	90
$	3000	0	0	0
MH	24	0	0	2

Probability of Overtemperature Effect		Probability of
Level 1	Level 2	Lightning Effect
-	-	-

Module Information Used by LCC

RDT&E $1.75 M

FAFTEEC Module: BLD2 Drive

Module Information Used by GRAMP

Constant Failure Rate	Abort Rate	Unit Cost	Unit Weight
38.6	19.3	2125	2.1

Module Information Used by GRAMS

Nonconstant Failure Rate (if appropriate)	Max. Operating Time	Unit Cost	Unit Weight
-	-	2125	2.1

		Typical Repair		
Category	At Depot	At Base	At Flightline	On Aircraft
%	100	-	-	-
$	450	0	0	0
MH	16	0	0	0

Probability of Overtemperature Effect		Probability of
Level 1	Level 2	Lightning Effect
-	-	.001

Module Information Used by LCC

RDT&E $.125 M

FAFTEEC Module: BLD2 Actuator

Module Information Used by GRAMP

Constant Failure Rate	Abort Rate	Unit Cost	Unit Weight
500	250	20000	30.0

Module Information Used by GRAMS

Nonconstant Failure Rate (if appropriate)	Max. Operating Time	Unit Cost	Unit Weight
Weibull: = 1577 = 2.05	150[illegible]	20000	30.0

Typical Repair

Category	At Depot	At Base	At Flightline	On Aircraft
%	95	0	0	5
$	2000	0	0	0
MH	40	0	0	4

Probability of Overtemperature Effect Level 1	Probability of Overtemperature Effect Level 2	Probability of Lightning Effect
-	-	-

Module Information Used by LCC

RDT&E $1.5 M

FAFTEEC Module: A8 Drive

Module Information Used by GRAMP

Constant Failure Rate	Abort Rate	Unit Cost	Unit Weight
39.9	39.9	2250	2.1

Module Information Used by GRAMS

Nonconstant Failure Rate (if appropriate)	Max. Operating Time	Unit Cost	Unit Weight
-	-	2250	2.1

Typical Repair

Category	At Depot	At Base	At Flightline	On Aircraft
%	100	-	-	-
$	450	0	0	0
MH	16	0	0	0

Probability of Overtemperature Effect Level 1	Probability of Overtemperature Effect Level 2	Probability of Lightning Effect
-	-	.001

Module Information Used by LCC

RDT&E $.125 M

FAFTEEC Module: A8 Actuator

Module Information Used by GRAMP

Constant Failure Rate	Abort Rate	Unit Cost	Unit Weight
500	250	25000	50.0

Module Information Used by GRAMS

Nonconstant Failure Rate (if appropriate)	Max. Operating Time	Unit Cost	Unit Weight
Weibull: = 1577 = 2.05	1500	25000	50.0

		Typical Repair		
Category	At Depot	At Base	At Flightline	On Aircraft
%	95	0	0	5
$	2000	0	0	0
MH	40	0	0	4

Probability of Overtemperature Effect		Probability of
Level 1	Level 2	Lightning Effect
-	-	-

Module Information Used by LCC

RDT&E $3.0 M

FAFTEEC Module: BLD1 Drive

Module Information Used by GRAMP

Constant Failure Rate	Abort Rate	Unit Cost	Unit Weight
401.3	0	4720	14.8

Module Information Used by GRAMS

Nonconstant Failure Rate (if appropriate)	Max. Operating Time	Unit Cost	Unit Weight
-	-	4720	14.8

		Typical Repair		
Category	At Depot	At Base	At Flightline	On Aircraft
%	100	-	-	-
$	940	0	0	0
MH	16	0	0	0

Probability of Overtemperature Effect		Probability of
Level 1	Level 2	Lightning Effect
-	-	.001

Module Information Used by LCC

RDT&E $.500 M

FAFTEEC Module: Speed Sensor

Module Information Used by GRAMP

Constant Failure Rate	Abort Rate	Unit Cost	Unit Weight
12.1	12.1	1000	1.7

Module Information Used by GRAMS

Nonconstant Failure Rate (if appropriate)	Max. Operating Time	Unit Cost	Unit Weight
-	-	1000	1.7

		Typical Repair		
Category	At Depot	At Base	At Flightline	On Aircraft
%	100	-	-	-
$	200	0	0	0
MH	4	0	0	0

Probability of Overtemperature Effect		Probability of
Level 1	Level 2	Lightning Effect
-	-	-

Module Information Used by LCC

RDT&E	$.100 M

FAFTEEC Module: CIT Sensor

Module Information Used by GRAMP

Constant Failure Rate	Abort Rate	Unit Cost	Unit Weight
40.4	40.4	875	1.1

Module Information Used by GRAMS

Nonconstant Failure Rate (if appropriate)	Max. Operating Time	Unit Cost	Unit Weight
-	5000	875	1.1

		Typical Repair		
Category	At Depot	At Base	At Flightline	On Aircraft
%	10	45	0	45
$	70	100	0	0
MH	8	4	0	.5

Probability of Overtemperature Effect		Probability of
Level 1	Level 2	Lightning Effect
-	-	-

Module Information Used by LCC

RDT&E	$.125 M

FAFTEEC Module: CDT Sensor

Module Information Used by GRAMP

Constant Failure Rate	Abort Rate	Unit Cost	Unit Weight
40.4	40.4	875	1.6

Module Information Used by GRAMS

Nonconstant Failure Rate (if appropriate)	Max. Operating Time	Unit Cost	Unit Weight
-	5000	875	1.6

Typical Repair

Category	At Depot	At Base	At Flightline	On Aircraft
%	10	45	0	45
$	70	100	0	0
MH	8	4	0	.5

Probability of Overtemperature Effect Level 1	Probability of Overtemperature Effect Level 2	Probability of Lightning Effect
-	-	-

Module Information Used by LCC

RDT&E $.050 M

FAFTEEC Module: EGT Sensor

Module Information Used by GRAMP

Constant Failure Rate	Abort Rate	Unit Cost	Unit Weight
40.4	40.4	3375	3.1

Module Information Used by GRAMS

Nonconstant Failure Rate (if appropriate)	Max. Operating Time	Unit Cost	Unit Weight
-	5000	3375	3.1

Typical Repair

Category	At Depot	At Base	At Flightline	On Aircraft
%	10	45	0	45
$	70	600	0	0
MH	8	4	0	.5

Probability of Overtemperature Effect Level 1	Probability of Overtemperature Effect Level 2	Probability of Lightning Effect
.0001	.001	-

Module Information Used by LCC

RDT&E $.050 M

FAFTEEC Module: TNOZ Sensor

Module Information Used by GRAMP

Constant Failure Rate	Abort Rate	Unit Cost	Unit Weight
40.4	0	1375	2.1

Module Information Used by GRAMS

Nonconstant Failure Rate (if appropriate)	Max. Operating Time	Unit Cost	Unit Weight
-	5000	1375	2.1

		Typical Repair		
Category	At Depot	At Base	At Flightline	On Aircraft
%	10	45	0	45
$	70	200	0	0
MH	8	4	0	.5

Probability of Overtemperature Effect		Probability of
Level 1	Level 2	Lightning Effect
.0001	.001	-

Module Information Used by LCC

RDT&E $.500 M

FAFTEEC Module: CIP Sensor

Module Information Used by GRAMP

Constant Failure Rate	Abort Rate	Unit Cost	Unit Weight
8.2	8.2	1750	3.3

Module Information Used by GRAMS

Nonconstant Failure Rate (if appropriate)	Max. Operating Time	Unit Cost	Unit Weight
-	-	1750	3.3

		Typical Repair		
Category	At Depot	At Base	At Flightline	On Aircraft
%	100	-	-	-
$	700	0	0	0
MH	24	0	0	0

Probability of Overtemperature Effect		Probability of
Level 1	Level 2	Lightning Effect
-	-	-

Module Information Used by LCC

RDT&E $2.5 M

FAFTEEC Module: P Sensor

Module Information Used by GRAMP

Constant Failure Rate	Abort Rate	Unit Cost	Unit Weight
8.2	8.2	1750	3.3

Module Information Used by GRAMS

Nonconstant Failure Rate (if appropriate)	Max. Operating Time	Unit Cost	Unit Weight
-	-	1750	3.3

		Typical Repair		
Category	At Depot	At Base	At Flightline	On Aircraft
%	100	-	-	-
$	200	0	0	0
MH	24	0	0	0

Probability of Overtemperature Effect		Probability of
Level 1	Level 2	Lightning Effect
-	-	-

Module Information Used by LCC

RDT&E $5.0 M

FAFTEEC Module: CDP Sensor

Module Information Used by GRAMP

Constant Failure Rate	Abort Rate	Unit Cost	Unit Weight
8.2	8.2	1750	2.3

Module Information Used by GRAMS

Nonconstant Failure Rate (if appropriate)	Max. Operating Time	Unit Cost	Unit Weight
-	-	1750	2.3

		Typical Repair		
Category	At Depot	At Base	At Flightline	On Aircraft
%	100	-	-	-
$	200	0	0	0
MH	24	0	0	0

Probability of Overtemperature Effect		Probability of
Level 1	Level 2	Lightning Effect
-	-	-

Module Information Used by LCC

RDT&E $2.5 M

FAFTEEC Module: EGP Sensor

Module Information Used by GRAMP

Constant Failure Rate	Abort Rate	Unit Cost	Unit Weight
8.2	8.2	1750	4.3

Module Information Used by GRAMS

Nonconstant Failure Rate (if appropriate)	Max. Operating Time	Unit Cost	Unit Weight
-	-	1750	4.3

		Typical Repair		
Category	At Depot	At Base	At Flightline	On Aircraft
%	100	-	-	-
$	200	0	0	0
MH	24	0	0	0

Probability of Overtemperature Effect		Probability of Lightning Effect
Level 1	Level 2	
.0001	.001	-

Module Information Used by LCC

RDT&E $2.5 M

FAFTEEC Module: WFA Sensor

Module Information Used by GRAMP

Constant Failure Rate	Abort Rate	Unit Cost	Unit Weight
22.7	7.7	1250	1.1

Module Information Used by GRAMS

Nonconstant Failure Rate (if appropriate)	Max. Operating Time	Unit Cost	Unit Weight
-	-	1250	1.1

		Typical Repair		
Category	At Depot	At Base	At Flightline	On Aircraft
%	100	-	-	-
$	250	0	0	0
MH	16	0	0	0

Probability of Overtemperature Effect		Probability of Lightning Effect
Level 1	Level 2	
-	-	.001

Module Information Used by LCC

RDT&E $.050 M

FAFTEEC Module: WFB Sensor

Module Information Used by GRAMP

Constant Failure Rate	Abort Rate	Unit Cost	Unit Weight
22.7	7.7	1250	1.1

Module Information Used by GRAMS

Nonconstant Failure Rate (if appropriate)	Max. Operating Time	Unit Cost	Unit Weight
-	-	1250	1.1

		Typical Repair		
Category	At Depot	At Base	At Flightline	On Aircraft
%	100	-	-	-
$	250	0	0	0
MH	16	0	0	0

Probability of Overtemperature Effect		Probability of
Level 1	Level 2	Lightning Effect
-	-	.001

Module Information Used by LCC

RDT&E $.050 M

FAFTEEC Module: A8 Sensor

Module Information Used by GRAMP

Constant Failure Rate	Abort Rate	Unit Cost	Unit Weight
22.7	0	1250	1.1

Module Information Used by GRAMS

Nonconstant Failure Rate (if appropriate)	Max. Operating Time	Unit Cost	Unit Weight
-	-	1250	1.1

		Typical Repair		
Category	At Depot	At Base	At Flightline	On Aircraft
%	100	-	-	-
$	250	0	0	0
MH	16	0	0	0

Probability of Overtemperature Effect		Probability of
Level 1	Level 2	Lightning Effect
-	-	.001

Module Information Used by LCC

RDT&E $.050 M

FAFTEEC Module: HPT Sensor

Module Information Used by GRAMP

Constant Failure Rate	Abort Rate	Unit Cost	Unit Weight
22.7	0	1250	1.1

Module Information Used by GRAMS

Nonconstant Failure Rate (if appropriate)	Max. Operating Time	Unit Cost	Unit Weight
-	-	1250	1.1

		Typical Repair		
Category	At Depot	At Base	At Flightline	On Aircraft
%	100	-	-	-
$	250	0	0	0
MH	16	0	0	0

Probability of Overtemperature Effect		Probability of
Level 1	Level 2	Lightning Effect
-	-	.001

Module Information Used by LCC

RDT&E $.050 M

FAFTEEC Module: BLD2 Sensor

Module Information Used by GRAMP

Constant Failure Rate	Abort Rate	Unit Cost	Unit Weight
22.7	12.7	1250	1.1

Module Information Used by GRAMS

Nonconstant Failure Rate (if appropriate)	Max. Operating Time	Unit Cost	Unit Weight
-	-	1250	1.1

		Typical Repair		
Category	At Depot	At Base	At Flightline	On Aircraft
%	100	-	-	-
$	250	0	0	0
MH	16	0	0	0

Probability of Overtemperature Effect		Probability of
Level 1	Level 2	Lightning Effect
-	-	.001

Module Information Used by LCC

RDT&E $.050 M

FAFTEEC Module: HPC Sensor

Module Information Used by GRAMP

Constant Failure Rate	Abort Rate	Unit Cost	Unit Weight
22.7	12.7	1250	1.1

Module Information Used by GRAMS

Nonconstant Failure Rate (if appropriate)	Max. Operating Time	Unit Cost	Unit Weight
-	-	1250	1.1

		Typical Repair		
Category	At Depot	At Base	At Flightline	On Aircraft
%	100	-	-	-
$	250	0	0	0
MH	16	0	0	0

Probability of Overtemperature Effect		Probability of
Level 1	Level 2	Lightning Effect
-	-	.001

Module Information Used by LCC

RDT&E $.050 M

FAFTEEC Module: Exciter/Igniter

Module Information Used by GRAMP

Constant Failure Rate	Abort Rate	Unit Cost	Unit Weight
88.3	15.0	3930	8.7

Module Information Used by GRAMS

Nonconstant Failure Rate (if appropriate)	Max. Operating Time	Unit Cost	Unit Weight
-	2000	3930	8.7

		Typical Repair		
Category	At Depot	At Base	At Flightline	On Aircraft
%	100	-	-	-
$	780	0	0	0
MH	16	0	0	0

Probability of Overtemperature Effect		Probability of
Level 1	Level 2	Lightning Effect
-	-	.001

Module Information Used by LCC

RDT&E $.125 M

FAFTEEC Module: Airstart

Module Information Used by GRAMP

Constant Failure Rate	Abort Rate	Unit Cost	Unit Weight
20.3	3.7	1430	3.7

Module Information Used by GRAMS

Nonconstant Failure Rate (if appropriate)	Max. Operating Time	Unit Cost	Unit Weight
-	-	1430	3.7

		Typical Repair		
Category	At Depot	At Base	At Flightline	On Aircraft
%	100	-	-	-
$	280	0	0	0
MH	16	0	0	0

Probability of Overtemperature Effect		Probability of
Level 1	Level 2	Lightning Effect
-	-	.001

Module Information Used by LCC

RDT&E $.125 M

FAFTEEC Module: De-Ice

Module Information Used by GRAMP

Constant Failure Rate	Abort Rate	Unit Cost	Unit Weight
20.3	0	1430	3.7

Module Information Used by GRAMS

Nonconstant Failure Rate (if appropriate)	Max. Operating Time	Unit Cost	Unit Weight
-	-	1430	3.7

		Typical Repair		
Category	At Depot	At Base	At Flightline	On Aircraft
%	100	-	-	-
$	280	0	0	0
MH	16	0	0	0

Probability of Overtemperature Effect		Probability of
Level 1	Level 2	Lightning Effect
-	-	.001

Module Information Used by LCC

RDT&E $.075 M

FAFTEEC Module: PMA

Module Information Used by GRAMP

Constant Failure Rate	Abort Rate	Unit Cost	Unit Weight
129.1	47.4	2000	5.0

Module Information Used by GRAMS

Nonconstant Failure Rate (if appropriate)	Max. Operating Time	Unit Cost	Unit Weight
-	-	2000	5.0

		Typical Repair		
Category	At Depot	At Base	At Flightline	On Aircraft
%	50	50	0	0
$	400	400	0	0
MH	8	8	0	0

Probability of Overtemperature Effect		Probability of
Level 1	Level 2	Lightning Effect
-	-	-

Module Information Used by LCC

RDT&E $.500 M

FAFTEEC Module: Backup Transfer

Module Information Used by GRAMP

Constant Failure Rate	Abort Rate	Unit Cost	Unit Weight
20.3	0	1430	3.7

Module Information Used by GRAMS

Nonconstant Failure Rate (if appropriate)	Max. Operating Time	Unit Cost	Unit Weight
-	-	1430	3.7

		Typical Repair		
Category	At Depot	At Base	At Flightline	On Aircraft
%	100	-	-	-
$	280	0	0	0
MH	16	0	0	0

Probability of Overtemperature Effect		Probability of
Level 1	Level 2	Lightning Effect
-	-	.001

Module Information Used by LCC

RDT&E